



UNSW
SYDNEY

MATH1081 – Discrete Mathematics

Topic 2 – Number theory and relations

Lecture 2.01 – Divisibility and greatest common divisors

Lecturer: Dr Sean Gardiner – sean.gardiner@unsw.edu.au

Introduction to number theory and relations

Number theory is primarily concerned with the study of integers and subsets of the integers. So for this topic we will mostly be working with:

- The **integers** $\mathbb{Z} = \{\dots, -3, -2, -1, 0, 1, 2, 3, \dots\}$.
- The **positive integers** $\mathbb{Z}^+ = \{1, 2, 3, \dots\}$.
- The **natural numbers** $\mathbb{N} = \{0, 1, 2, 3, \dots\}$.

For these and all other number sets we have encountered (\mathbb{Q} , \mathbb{R} , \mathbb{C}), if we add or multiply any two elements from one of the sets, we attain another element from that set. But for the operation of division, the integers and its subsets are distinguished by the fact that this property does not hold – dividing one integer by another non-zero integer does not guarantee an integer result.

Number theory is one of the most fundamental branches of Mathematics, and is still relevant in the modern era especially considering its applications to cryptography.

Towards the end of this topic, we will also address the topic of mathematical relations, which is a natural generalisation of what we have already learned about functions, and provides more structure to our understanding of divisibility and modular arithmetic.

Divisibility

Definition. Given two integers a and b , we say a **divides** b if we can write $b = ak$ for some integer k . We might also say:

- a is a **divisor** of b ,
- a is a **factor** of b ,
- b is **divisible** by a , or
- b is a **multiple** of a .

Notation. The expression $a \mid b$ is read as “ a divides b ” and is equivalent to writing $b = ak$ for some integer k . The expression $a \nmid b$ is read as “ a does not divide b ”, and means that $b \neq ak$ for any integer k .

Example. Decide whether the following statements are true or false.

- $3 \mid 15$ is **true** since $15 = 3 \times 5$ and $5 \in \mathbb{Z}$.
- $15 \mid 3$ is **false** since $3 = 15 \times \frac{1}{5}$ but $\frac{1}{5} \notin \mathbb{Z}$.
- $3 \mid 3$ is **true** since $3 = 3 \times 1$ and $1 \in \mathbb{Z}$.
- $-5 \mid 15$ is **true** since $15 = (-5) \times (-3)$ and $-3 \in \mathbb{Z}$.
- $0 \mid 3$ is **false** since there is no integer k such that $3 = 0 \times k$.
- $3 \mid 0$ is **true** since $0 = 3 \times 0$ and $0 \in \mathbb{Z}$.
- $0 \mid 0$ is **true** since $0 = 0 \times 1$ (for example) and $1 \in \mathbb{Z}$.

Divisibility properties

The divisibility relation has many useful properties. Some of the most important are the following.

Lemma. For all integers a , we have $a \mid a$.

Proof. Since $a = a \times 1$ and $1 \in \mathbb{Z}$, we have by definition that $a \mid a$.

Lemma. For all integers a, b, c , if $a \mid b$ and $b \mid c$, then $a \mid c$.

Proof. Since $a \mid b$, we have $b = ak$ for some $k \in \mathbb{Z}$, and since $b \mid c$, we have $c = bl$ for some $l \in \mathbb{Z}$. So $c = (ak)l = a(kl)$ where $kl \in \mathbb{Z}$, so $a \mid c$.

Lemma. For all integers a, b, c , if $a \mid b$ and $a \mid c$, then $a \mid bx + cy$ for any $x, y \in \mathbb{Z}$.

Proof. Since $a \mid b$, we have $b = ak$ for some $k \in \mathbb{Z}$, and since $a \mid c$, we have $c = al$ for some $l \in \mathbb{Z}$. So $bx + cy = (ak)x + (al)y = a(kx + ly)$ where $kx + ly \in \mathbb{Z}$, so $a \mid bx + cy$.

We can deduce other useful facts from the above properties. For example, setting $c = 0$ in the third lemma shows that if $a \mid b$ then $a \mid bm$ for any integer m . Combining this with the first lemma shows that $a \mid am$ for any integer m .

Prime numbers

Definition. A **prime number** (or just a **prime**) is any $p \in \mathbb{N}$ such that $p > 1$ and the **only** positive divisors of p are 1 and p .

The first few prime numbers are 2, 3, 5, 7, 11, 13, 17, 19,

Definition. A **composite number** is any natural number that is not 0, 1, or a prime number.

The first few composite numbers are 4, 6, 8, 9, 10, 12,

Theorem. There are infinitely many prime numbers.

Proof. See Angell: Slide 3.53 (or Gardiner: Lecture 3.07, Example 5).

To determine if a natural number n is prime, a standard approach is to check whether it is divisible by all known primes less than or equal to \sqrt{n} . (See Problem Set 3, Question 25.)

For example, 1009 is prime because it is not divisible by any of the primes less than or equal to $\lfloor \sqrt{1009} \rfloor = 31$.

Fundamental Theorem of Arithmetic

Theorem. (Fundamental Theorem of Arithmetic)

Every natural number greater than 1 has a **unique prime factorisation**. That is, given any positive integer $n > 1$, it can be written uniquely in the form

$$n = p_1^{\alpha_1} p_2^{\alpha_2} p_3^{\alpha_3} \cdots p_k^{\alpha_k},$$

where each p_1, p_2, \dots, p_k is a prime number, $p_1 < p_2 < p_3 < \cdots < p_k$, and $\alpha_1, \alpha_2, \dots, \alpha_k \in \mathbb{Z}^+$ for some $k \in \mathbb{Z}^+$.

Proof. See Angell: Slide 3.76 (or Gardiner: Lecture 3.08, Example 4).

For example, the prime factorisation of 12 is $2^2 \times 3$.

Example. Find the prime factorisations for each of the integers from 21 to 25.

- $21 = 3 \times 7$.
- $22 = 2 \times 11$.
- $23 = 23$.
- $24 = 2^3 \times 3$.
- $25 = 5^2$.

Common divisors

Definition. A **common divisor** of two integers a and b is any integer d such that both $d \mid a$ and $d \mid b$.

Example. Which of the following are common divisors of 12 and 18?

- 1 **is** a common divisor of 12 and 18 because $1 \mid 12$ and $1 \mid 18$.
- -6 **is** a common divisor of 12 and 18 because $-6 \mid 12$ and $-6 \mid 18$.
- 9 is **not** a common divisor of 12 and 18 because $9 \mid 18$ but $9 \nmid 12$.

Definition. Two integers a and b are **coprime** or **relatively prime** if and only if their only common divisors are 1 and -1 . Equivalently, two integers are coprime if and only if their only positive common divisor is 1.

Example. Which of the following pairs of numbers are coprime?

- 2 and 3 **are** coprime because 1 is their only positive common divisor.
- 9 and -10 **are** coprime because 1 is their only positive common divisor.
- 12 and 18 are **not** coprime because they have positive common divisors other than 1, for example 2, 3, or 6.
- 0 and 1 **are** coprime because 1 is their only positive common divisor.

Greatest common divisors

Definition. The **greatest common divisor** (GCD) of two integers a and b (when a and b are not both 0), denoted $\gcd(a, b)$, is the natural number $d \in \mathbb{N}$ such that

- both $d \mid a$ and $d \mid b$, and
- for all $c \in \mathbb{N}$, if $c \mid a$ and $c \mid b$, then $c \leq d$.

For example, $\gcd(3, 5) = 1$ and $\gcd(12, 18) = 6$.

If the prime factorisations of a and b are known, then $\gcd(a, b)$ can easily be found by taking the product of the **lower powers of each prime factor**. For example, $\gcd(108, 72) = \gcd(2^2 \times 3^3, 2^3 \times 3^2) = 2^2 \times 3^2 = 36$.

Example. Find $\gcd(2^3 \times 3^2 \times 7, 2^2 \times 3 \times 5)$.

Solution. We have $\gcd(2^3 \times 3^2 \times 7, 2^2 \times 3 \times 5) = 2^2 \times 3^1 \times 5^0 \times 7^0 = 12$.

Alternate definition. The greatest common divisor $\gcd(a, b)$ of two integers a and b is the natural number $d \in \mathbb{N}$ such that

- both $d \mid a$ and $d \mid b$, and
- for all $c \in \mathbb{N}$, if $c \mid a$ and $c \mid b$, then $c \mid d$.

With this definition, the value of $\gcd(0, 0)$ is well-defined and equals 0.

Properties of the GCD

Some useful properties of the GCD are given below. Suppose a, b, c, q are integers.

- **Property 1.** $\gcd(a, 1) = 1$.
- **Property 2.** $\gcd(a, 0) = |a|$.
- **Property 3.** $\gcd(a, \gcd(b, c)) = \gcd(\gcd(a, b), c)$.
- **Property 4.** $\gcd(ac, bc) = |c| \gcd(a, b)$.
- **Property 5.** If $a \mid bc$ and $\gcd(a, b) = 1$, then $a \mid c$.
- **Property 6.** If $a = qb + c$, then $\gcd(a, b) = \gcd(b, c)$.

Proof. Since $a = qb + c$ and $\gcd(b, c)$ is a common divisor of b and c , it must also be a divisor of a (by the third lemma on slide 3). So $\gcd(b, c) \leq \gcd(a, b)$, since $\gcd(a, b)$ is the greatest common divisor of a and b .

Similarly, since $c = a - qb$ and $\gcd(a, b)$ is a common divisor of a and b , it must also be a divisor of c . So $\gcd(a, b) \leq \gcd(b, c)$, since $\gcd(b, c)$ is the greatest common divisor of b and c .

Combining both these inequations, we deduce that $\gcd(a, b) = \gcd(b, c)$.

Least common multiples

Definition. The **least common multiple** (LCM) of two non-zero integers a and b , denoted $\text{lcm}(a, b)$, is the positive integer $d \in \mathbb{Z}^+$ such that

- both $a \mid d$ and $b \mid d$, and
- for all $c \in \mathbb{Z}^+$, if $a \mid c$ and $b \mid c$, then $d \leq c$.

For example, $\text{lcm}(3, 5) = 15$, and $\text{lcm}(4, 6) = 12$.

If the prime factorisations of a and b are known, then $\text{lcm}(a, b)$ can easily be found by taking the product of the **higher powers of each prime factor**. For example, $\text{lcm}(108, 72) = \text{lcm}(2^2 \times 3^3, 2^3 \times 3^2) = 2^3 \times 3^3 = 216$.

Example. Find $\text{lcm}(2^3 \times 3^2 \times 7, 2^2 \times 3 \times 5)$.

Solution. We have $\text{lcm}(2^3 \times 3^2 \times 7, 2^2 \times 3 \times 5) = 2^3 \times 3^2 \times 5^1 \times 7^1 = 2520$.

Fact. For any positive integers a and b , we have $\text{gcd}(a, b) \text{lcm}(a, b) = ab$.

Alternate definition. The least common multiple $\text{lcm}(a, b)$ of two integers a and b is the natural number $d \in \mathbb{N}$ such that

- both $a \mid d$ and $b \mid d$, and
- for all $c \in \mathbb{N}$, if $a \mid c$ and $b \mid c$, then $d \mid c$.

With this definition, $\text{lcm}(a, b)$ is well-defined even when a or b is 0.

Case study: Natural numbers as sets

(Remember that “case studies” are additional content and not examinable.)

In the early 1920s, Ernst Zermelo and Abraham Fraenkel set out to describe set theory entirely axiomatically, meaning they wanted to rigorously define/prove all aspects of set theory using only a minimal list of assumed axioms (fundamental truths). Their motivation was to build up a system that avoided the construction paradoxes like Russell's paradox. The resulting so-called Zermelo-Fraenkel set theory is still used as the standard model for axiomatic set theory today.

Soon thereafter, at the age of 19, mathematician and computer scientist John von Neumann described a way of defining the natural numbers in the context of ZF set theory. The system defines the number 0 as being represented by the empty set, and for each positive integer n , the number $n + 1$ is defined by $n + 1 := n \cup \{n\}$. This construction allows the number n to be represented by the set with cardinality n .

$$\begin{array}{llll} 0 & := & \{\} & = & \{\} \\ 1 & := & \{0\} & = & \{\{\}\} \\ 2 & := & \{0,1\} & = & \{\{\},\{\{\}\}\} \\ 3 & := & \{0,1,2\} & = & \{\{\},\{\{\}\},\{\{\},\{\{\}\}\}\}. \end{array}$$



UNSW
SYDNEY

MATH1081 – Discrete Mathematics

Topic 2 – Number theory and relations

Lecture 2.02 – The Euclidean algorithm

Lecturer: Dr Sean Gardiner – sean.gardiner@unsw.edu.au

The Division Theorem

Theorem. (Division Theorem)

For any integers a and b with $b \neq 0$, there exist **unique** integers q and r such that both

$$a = qb + r \quad \text{and} \quad 0 \leq r < |b|.$$

We call q the **quotient** and r the **remainder** when a is divided by b .

Proof. See Angell: Slide 3.37 (or Gardiner: Lecture 3.04, Example 4).

Example. What is the quotient and remainder when...

- 30 is divided by 7?

Here $q = 4$ and $r = 2$, since $30 = 4 \times 7 + 2$ and $0 \leq 2 < 7$.

- 30 is divided by 6?

Here $q = 5$ and $r = 0$, since $30 = 5 \times 6 + 0$ and $0 \leq 0 < 6$.

- 30 is divided by -4 ?

Here $q = -7$ and $r = 2$, since $30 = (-7) \times (-4) + 2$ and $0 \leq 2 < |-4|$.

- -30 is divided by 4?

Here $q = -8$ and $r = 2$, since $-30 = (-8) \times 4 + 2$ and $0 \leq 2 < 4$.

The Euclidean algorithm

The **Euclidean algorithm** is a process that, given two integers a and $b \neq 0$ as inputs, efficiently finds $\gcd(a, b)$. The algorithm makes use of the Division Theorem, finding quotients and remainders iteratively in the following way:

$$\begin{array}{ll} a = q_0 \times b + r_0 & \text{where } q_0, r_0 \in \mathbb{Z} \text{ and } |b| > r_0 \geq 0, \\ b = q_1 \times r_0 + r_1 & \text{where } q_1, r_1 \in \mathbb{Z} \text{ and } r_0 > r_1 \geq 0, \\ r_0 = q_2 \times r_1 + r_2 & \text{where } q_2, r_2 \in \mathbb{Z} \text{ and } r_1 > r_2 \geq 0, \\ r_1 = q_3 \times r_2 + r_3 & \text{where } q_3, r_3 \in \mathbb{Z} \text{ and } r_2 > r_3 \geq 0, \\ \vdots & \vdots \\ r_{n-2} = q_n \times r_{n-1} + r_n & \text{where } q_n, r_n \in \mathbb{Z} \text{ and } r_{n-1} > r_n \geq 0, \\ r_{n-1} = q_{n+1} \times r_n + 0 & \text{where } q_{n+1} \in \mathbb{Z} \text{ and } r_n > 0. \end{array}$$

The process terminates immediately after the n th step, when the remainder is first found to be zero. The remainder at the n th step is then the GCD of a and b . That is,

$$\gcd(a, b) = r_n.$$

Example – Euclidean algorithm

Example. Use the Euclidean algorithm to find $\gcd(403, 286)$.

Solution. We have

$$403 = 1 \times 286 + 117,$$

$$286 = 2 \times 117 + 52,$$

$$117 = 2 \times 52 + 13,$$

$$52 = 4 \times 13 + 0.$$

So $\gcd(403, 286) = 13$.

Example. Use the Euclidean algorithm to find $\gcd(283, 193)$.

Solution. We have

$$283 = 1 \times 193 + 90,$$

$$193 = 2 \times 90 + 13,$$

$$90 = 6 \times 13 + 12,$$

$$13 = 1 \times 12 + 1,$$

$$12 = 12 \times 1 + 0.$$

So $\gcd(283, 193) = 1$. (That is, 283 and 193 are coprime.)

The Euclidean algorithm – proof

Theorem. For any integer inputs a and $b \neq 0$, the Euclidean algorithm always outputs $\gcd(a, b)$.

Proof. To prove this is true, we need to show that the process always terminates, and always returns the GCD.

As a reminder, the first few steps of the Euclidean algorithm for a and b are:

$$\begin{array}{ll} a = q_0 \times b + r_0 & \text{where } q_0, r_0 \in \mathbb{N} \text{ and } |b| > r_0 \geq 0, \\ b = q_1 \times r_0 + r_1 & \text{where } q_1, r_1 \in \mathbb{N} \text{ and } r_0 > r_1 \geq 0, \\ r_0 = q_2 \times r_1 + r_2 & \text{where } q_2, r_2 \in \mathbb{N} \text{ and } r_1 > r_2 \geq 0 \dots \end{array}$$

Notice that the process must eventually terminate, since we have $|b| > r_0 > r_1 > \dots \geq 0$, so the remainders are strictly decreasing, and must eventually reach zero after at most $|b|$ steps.

Notice also that $\gcd(a, b) = \gcd(b, r_0)$, by Property 6 from Lecture 2.01. Similarly, $\gcd(b, r_0) = \gcd(r_0, r_1)$, and so on. So in particular, if the algorithm terminates after n steps (so the remainder $r_{n+1} = 0$), we have that $\gcd(a, b) = \gcd(b, r_0) = \gcd(r_0, r_1) = \dots = \gcd(r_{n-1}, r_n) = \gcd(r_n, 0)$. Recall also that $\gcd(r_n, 0) = r_n$, so the output of the Euclidean algorithm really is $\gcd(a, b)$.

Euclidean algorithm in reverse

Recall the Euclidean algorithm applied to 286 and 403 as follows:

$$403 = 1 \times 286 + 117, \quad \textcircled{1}$$

$$286 = 2 \times 117 + 52, \quad \textcircled{2}$$

$$117 = 2 \times 52 + 13, \quad \textcircled{3}$$

$$52 = 4 \times 13 + 0.$$

Notice that **working backwards** from the penultimate line, it should be possible to make careful substitutions so that we can eventually express $\gcd(403, 286)$ as an integer linear combination of 403 and 286:

$$\begin{aligned} 13 &= 117 - 2 \times 52 && \text{(from } \textcircled{3}) \\ &= 117 - 2 \times (286 - 2 \times 117) && \text{(substituting from } \textcircled{2}) \\ &= 5 \times 117 - 2 \times 286 && \text{(collecting terms)} \\ &= 5 \times (403 - 286) - 2 \times 286 && \text{(substituting from } \textcircled{1}) \\ &= 5 \times 403 - 7 \times 286 && \text{(collecting terms).} \end{aligned}$$

So we can write $\gcd(403, 286)$ in the form $403x + 286y$ for integers x and y , where specifically $x = 5$ and $y = -7$.

Bézout's identity

The method we just saw can be generalised for any pair of integers.

Theorem. (Bézout's identity)

Given any integers a and b , there exist integers x and y such that

$$\gcd(a, b) = ax + by.$$

Values for x and y can be found by applying the Euclidean algorithm to a and b and then working backwards, like in the previous example.

Note that the solution pair (x, y) is not unique. For example, we saw $\gcd(403, 286) = 13 = 5 \times 403 + (-7) \times 286$, but it is also true that $\gcd(403, 286) = 13 = (-17) \times 403 + 24 \times 286$.

Notice that Bézout's identity cannot be used in reverse. However, the following weaker statement is true.

Theorem. Given $d = ax + by$ for some integers a, b, x, y , we have that

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

Proof. By definition, $\gcd(a, b) \mid a$ and $\gcd(a, b) \mid b$. So $\gcd(a, b)$ must be a divisor of any integer linear combination of a and b , by a previous result about divisibility.

Example – Bézout's identity

Example. Find integers x and y such that $\gcd(283, 193) = 283x + 193y$.

Solution. The Euclidean algorithm applied to 283 and 193 gives:

$$283 = 1 \times 193 + 90,$$

$$193 = 2 \times 90 + 13,$$

$$90 = 6 \times 13 + 12,$$

$$13 = 1 \times 12 + 1,$$

$$12 = 12 \times 1 + 0.$$

Working backwards from the penultimate line, we get:

$$1 = 13 - 12$$

$$= 13 - (90 - 6 \times 13)$$

$$= 7 \times 13 - 90$$

$$= 7 \times (193 - 2 \times 90) - 90$$

$$= 7 \times 193 - 15 \times 90$$

$$= 7 \times 193 - 15 \times (283 - 193)$$

$$= 22 \times 193 - 15 \times 283.$$

So $\gcd(283, 193) = 1 = 22 \times 193 - 15 \times 283$, that is, $x = -15$ and $y = 22$.

Solving linear equations for integers

Theorem. Given integers a , b , and c , there exist integers x and y such that $ax + by = c$ if and only if $\gcd(a, b) \mid c$.

Proof. First suppose $ax + by = c$ for some integers x and y . Since $\gcd(a, b)$ is a divisor of both a and b , we must have that $\gcd(a, b) \mid (ax + by)$ for all integers x, y . So $\gcd(a, b) \mid c$.

Next suppose $\gcd(a, b) \mid c$. Then $c = \gcd(a, b)k$ for some integer k . By Bézout's identity, we know there exist integers x' and y' such that $\gcd(a, b) = ax' + by'$. Multiplying through by k then gives $c = a(kx') + b(ky')$ where $x = kx'$ and $y = ky'$ are integers.

Corollary. Suppose we are given integers a , b , and c , and wish to solve $ax + by = c$ for integers x and y .

- If $\gcd(a, b) \nmid c$, then there are no integer solutions.
- If $\gcd(a, b) \mid c$, then we can find integer solutions as follows:
 - Find integers x' and y' satisfying $ax' + by' = \gcd(a, b)$ by applying the Euclidean algorithm to a and b and working backwards.
 - Writing $d = \gcd(a, b)$, we have that $x = \frac{c}{d}x'$ and $y = \frac{c}{d}y'$ are integer solutions to $ax + by = c$.

Example – Solving linear equations for integers

Example. Find integers x and y such that $289x + 119y = 13$.

Solution. The Euclidean algorithm applied to 289 and 119 gives:

$$289 = 2 \times 119 + 51,$$

$$119 = 2 \times 51 + 17,$$

$$51 = 3 \times 17 + 0.$$

So $\gcd(289, 119) = 17$, which does not divide 13. Thus there are no integer solutions to $289x + 119y = 13$.

Example. Find integers x and y such that $289x + 119y = 34$.

Solution. In this case, $\gcd(289, 119) = 17$ is a divisor of 34, so there do exist integer solutions.

Working backwards from the penultimate line of the Euclidean algorithm:

$$\begin{aligned} 17 &= 119 - 2 \times 51 \\ &= 119 - 2(289 - 2 \times 119) \\ &= 5 \times 119 - 2 \times 289. \end{aligned}$$

So an integer solution to $17 = 289x' + 119y'$ is $x' = -2$ and $y' = 5$.

Thus an integer solution to $34 = 289x + 119y$ is $x = -4$ and $y = 10$.

Using Bézout's identity in proofs

When proving statements involving GCDs, it can often be useful to use Bézout's identity. That is, if we are given that $\gcd(a, b) = c$, then we can use the fact that $c = ax + by$ for some $x, y \in \mathbb{Z}$.

For example, consider the following applications:

Theorem. Suppose a , b , and c are integers with $a \mid bc$ and $\gcd(a, b) = 1$. Then $a \mid c$.

Proof. Since $a \mid bc$, we may write $bc = ak$ for some integer k . Since $\gcd(a, b) = 1$, by Bézout's identity there exist integers x and y such that $1 = ax + by$. Multiplying this through by c gives

$$c = acx + bcy = acx + ak y = a(cx + ky).$$

Since $cx + ky$ is an integer, we can conclude that $a \mid c$.

Exercise. Suppose a and b are integers and p is a prime number. Prove that if $p \mid ab$, then $p \mid a$ or $p \mid b$.

Proof. (See Problem Set 3, Question 28.)

This property of prime numbers is actually the way prime elements are generally defined.



UNSW
SYDNEY

MATH1081 – Discrete Mathematics

Topic 2 – Number theory and relations

Lecture 2.03 – Modular arithmetic

Lecturer: Dr Sean Gardiner – sean.gardiner@unsw.edu.au

The mod operator

Recall the **Division Theorem** states that for any integers a and b with $b \neq 0$, there exist unique integers q and r such that both

$$a = qb + r \quad \text{and} \quad 0 \leq r < |b|.$$

In many situations, we are particularly interested in the **remainder** r .

Notation. The modulo operator **mod** returns the canonical remainder when one integer is divided by another. We write $a \bmod b$, read as “ a modulo b ”, to mean the (smallest non-negative) remainder when a is divided by b . That is, given integers a and b with $b \neq 0$, we have $a \bmod b = r$ where $0 \leq r < |b|$ and $a = qb + r$ for some $q, r \in \mathbb{Z}$.

Example. Find the following values:

- $19 \bmod 4 = 3$.
- $-11 \bmod 5 = 4$.
- $333 \bmod 3 = 0$.

Notice that $a \bmod b = 0$ if and only if $b \mid a$.

In most computer programming languages, the mod operator is represented by the character `%`. However, this symbol is never used for this purpose in mathematical texts.

Modular congruence

We saw that $19 \bmod 4 = 3$, and of course there are infinitely many integers x such that $x \bmod 4 = 3$. We can think of all such numbers as having something in common, and say they belong to the same **equivalence class**. Instead of writing (for example) $19 \bmod 4 = 47 \bmod 4$, we can use a special congruence notation $19 \equiv 47 \pmod{4}$.

Notation. Given integers a and b and a positive integer m , we say that a and b are **congruent modulo m** and write $a \equiv b \pmod{m}$ to mean that $a \bmod m = b \bmod m$.

The following are all equivalent statements:

- $a \equiv b \pmod{m}$.
- $a \bmod m = b \bmod m$.
- a and b have the same remainder when divided by m .
- $a = b + mk$ for some integer k .
- $m \mid (a - b)$.

Challenge. Prove the above statements are equivalent.

Properties of modular arithmetic

Suppose $a, b, c, d \in \mathbb{Z}$ and $m \in \mathbb{Z}^+$. Below are several useful properties of modular arithmetic:

- If $a \equiv b \pmod{m}$, and $k \in \mathbb{Z}^+$ satisfies $k \mid m$, then $a \equiv b \pmod{k}$.
- If $a \equiv b \pmod{m}$ and $c \equiv d \pmod{m}$, then $a + c \equiv b + d \pmod{m}$.
- If $a \equiv b \pmod{m}$, then $a + k \equiv b + k \pmod{m}$ for all $k \in \mathbb{Z}$.
- If $a \equiv b \pmod{m}$ and $c \equiv d \pmod{m}$, then $ac \equiv bd \pmod{m}$.
- If $a \equiv b \pmod{m}$, then $ak \equiv bk \pmod{m}$ for all $k \in \mathbb{Z}$.
- If $a \equiv b \pmod{m}$, then $ak \equiv bk \pmod{mk}$ for all $k \in \mathbb{Z}^+$.
- If $ak \equiv bk \pmod{mk}$ for some $k \in \mathbb{Z}^+$, then $a \equiv b \pmod{m}$.

(If there is a divisor common to both sides of the congruence and the modulus, we can “divide” all terms through by that common divisor.)

- If $ak \equiv bk \pmod{m}$ for some $k \in \mathbb{Z}$, and $\gcd(m, k) = 1$, then $a \equiv b \pmod{m}$.

(If there is a divisor common to both sides of the congruence and it is coprime with the modulus, we can “divide” both sides of the congruence through by that common divisor.)

- If $a \equiv b \pmod{m}$, then $a^k \equiv b^k \pmod{m}$ for all $k \in \mathbb{Z}^+$.

Properties of modular arithmetic – Proofs

Proofs are provided for two of these properties...

Theorem. If $a \equiv b \pmod{m}$ and $c \equiv d \pmod{m}$, then $ac \equiv bd \pmod{m}$.

Proof. Since $a \equiv b \pmod{m}$, we know that $a = b + mk$ for some integer k , and since $c \equiv d \pmod{m}$, we know $c = d + ml$ for some integer l . So $ac = (b + mk)(d + ml) = bd + mbl + mdk + m^2kl = bd + m(bl + dk + mkl)$ where $bl + dk + mkl \in \mathbb{Z}$. Thus $ac \equiv bd \pmod{m}$.

Theorem. If $ak \equiv bk \pmod{m}$ for some $k \in \mathbb{Z}$, and $\gcd(m, k) = 1$, then $a \equiv b \pmod{m}$.

Proof. Since $ak \equiv bk \pmod{m}$, we know that $m \mid (ak - bk)$, so $m \mid k(a - b)$. By the GCD Property 5 from Lecture 2.01, since $\gcd(m, k) = 1$, we must have that $m \mid (a - b)$, which is equivalent to saying $a \equiv b \pmod{m}$.

Challenge. Using similar approaches, prove that the other properties hold.

Similar problems appear in Problem Set 2, Questions 6 and 8.

Problem-solving with modular arithmetic

Having established these properties of modular arithmetic, we now have a useful set of tools for solving problems that involve divisibility or remainders.

Example. Prove that a natural number is divisible by 3 if and only if its digit sum is divisible by 3.

Solution. Let n be any natural number with $k + 1$ digits $d_0, d_1, d_2, \dots, d_k$ from right to left, so that

$$n = 10^0 d_0 + 10^1 d_1 + 10^2 d_2 + \cdots + 10^k d_k$$

where each d_i is an integer between 0 and 9 inclusive. Then working modulo 3, since $10 \bmod 3 = 1$, we have

$$\begin{aligned} n &= 10^0 d_0 + 10^1 d_1 + 10^2 d_2 + \cdots + 10^k d_k \\ &\equiv 1^0 d_0 + 1^1 d_1 + 1^2 d_2 + \cdots + 1^k d_k \pmod{3} \\ &\equiv d_0 + d_1 + d_2 + \cdots + d_k \pmod{3}. \end{aligned}$$

Thus n has the same residue modulo 3 as its digit sum. So in particular, $n \bmod 3 = 0$ if and only if n 's digit sum is congruent to 0 modulo 3, meaning n is divisible by 3 if and only if its digit sum is divisible by 3.

Reducing powers modulo m

Finding large powers of the form a^k modulo m can be difficult, since while we are allowed to reduce a modulo m , we cannot reduce the power k in the same way. However, it is always possible to simplify the expression by finding small powers of a that reduce to smaller values modulo m , helping to decrease the value of a^k in steps. Typically, we look for a small power of a that is close to 0 (ideally 1 or -1) modulo m .

Example. Find $7^{1001} \bmod 12$.

Solution. Checking small powers of 7, we first find that $7^2 \equiv 49 \equiv 1 \pmod{12}$. So we have

$$7^{1001} \equiv (7^2)^{500} \times 7^1 \equiv 1^{500} \times 7 \equiv 7 \pmod{12},$$

meaning $7^{1001} \bmod 12 = 7$.

Example. Find $12^{1001} \bmod 7$.

Solution. First we can note that $12^{1001} \equiv (-2)^{1001} \pmod{7}$. Checking small powers of 2, we find that $(-2)^3 = -8 \equiv -1 \pmod{7}$, so

$$(-2)^{1001} \equiv ((-2)^3)^{333} \times (-2)^2 \equiv (-1)^{333} \times 4 \equiv -4 \equiv 3 \pmod{7}.$$

Thus $12^{1001} \bmod 7 = 3$.

Reducing powers modulo m – Example 2

Example. Find $5^{1001} \bmod 93$.

Solution. In order to check small powers of 5 here, it can be useful to use a table. Working modulo 93, we have:

n	1	2	3	4	5	6	...
5^n	5	25	32	-26	-37	1	...

Notice that to find each entry in this table, we only needed to multiply the previous entry by 5 and reduce the result modulo 93. To keep the multiplications manageable, we can always choose to use the reduced value that is closest to 0. For example, to find 5^4 modulo 93, we did the following:

$$5^4 = 5^3 \times 5 \equiv 32 \times 5 \equiv 160 \equiv 67 \equiv -26 \pmod{93}.$$

Seeing that $5^6 \equiv 1 \pmod{93}$, we can deduce that

$$5^{1001} \equiv (5^6)^{166} \times 5^5 \equiv 1^{166} \times (-37) \equiv -37 \equiv 56 \pmod{93}.$$

That is, $5^{1001} \bmod 93 = 56$.

Reducing powers modulo m – Example 3

Example. Find $3^{103} \bmod 15$.

Solution. We can again check small powers of 3 here, working modulo 15:

n	1	2	3	4	5	...
3^n	3	9	12	6	3	...

In this case, we can see we will never encounter a power of 3 that gives 1 modulo 15. But we can also see that the powers of 3 modulo 15 repeat with period 4. So $3 \equiv 3^5 \equiv 3^9 \equiv 3^{13} \equiv \dots \equiv 3^{101} \pmod{15}$, and thus

$$3^{103} \equiv 3^{101} \times 3^2 \equiv 3 \times 9 \equiv 27 \equiv 12 \pmod{15}.$$

Alternate solution. We can divide both the value and its modulus by the common factor of 3 and first find $3^{102} \bmod 5$. In this case, we can notice that $3^2 = 9 \equiv -1 \pmod{5}$, so

$$3^{102} \equiv (3^2)^{51} \equiv (-1)^{51} \equiv -1 \equiv 4 \pmod{5}.$$

So $3^{102} \equiv 4 \pmod{5}$, and we can now multiply both sides of the congruence and the modulus through by 3 to find $3^{103} \equiv 12 \pmod{15}$.

Fermat's Little Theorem

A useful theorem for simplifying powers in prime moduli is Fermat's Little Theorem:

Theorem. (Fermat's Little Theorem)

For any prime p and any integer a such that $p \nmid a$, we have

$$a^{p-1} \equiv 1 \pmod{p}.$$

Proof. (See MATH2400 – Finite Mathematics!)

Note that $p - 1$ is **not** necessarily the smallest non-negative power of a that is 1 modulo p .

Example. Find the following values.

- $99^{100} \bmod 101$.

Solution. Since 101 is prime, by FLT, $a^{100} \equiv 1 \pmod{101}$ for all integers a where $101 \nmid a$. So in this case we must have $99^{100} \bmod 101 = 1$.

- $99^{909} \bmod 101$.

Solution. We just showed that $99^{100} \bmod 101 = 1$, so

$$99^{909} = (99^{100})^9 \times 99^9 \equiv 1 \times (-2)^9 \equiv -512 \equiv 94 \pmod{101}.$$



UNSW
SYDNEY

MATH1081 – Discrete Mathematics

Topic 2 – Number theory and relations

Lecture 2.04 – Solving linear modular congruences

Lecturer: Dr Sean Gardiner – sean.gardiner@unsw.edu.au

Linear congruences

Definition. A **linear congruence** is an expression of the form $ax \equiv c \pmod{m}$ for given integers a , c , and m . Note that this expression only makes sense if the unknown x is also an integer.

A linear congruence can have no solutions or infinitely many solutions, which can be expressed together as values in certain moduli. We shall investigate this in more detail on the next slides.

Notice that the linear equation $ax + my = c$, when considered modulo m , becomes the linear congruence

$$ax + my \equiv c \pmod{m},$$

$$ax + 0y \equiv c \pmod{m},$$

$$ax \equiv c \pmod{m}.$$

In fact, the solutions to $ax \equiv c \pmod{m}$ are precisely the integer x -values that solve $ax + my = c$ for integers x and y . So what we have learned about solving integer linear equations will also have applications when solving linear congruences.

Linear congruences – Checking all multiples

Example. Find all solutions to the linear congruence $6x \equiv 4 \pmod{7}$.

Solution. Checking the multiples of 6 while working modulo 7, we have:

x	0	1	2	3	4	5	6
$6x$	0	6	5	4	3	2	1

So the only solution is $x \equiv 3 \pmod{7}$.

Example. Find all solutions to the linear congruence $6x \equiv 4 \pmod{8}$.

Solution. Checking the multiples of 6 while working modulo 8, we have:

x	0	1	2	3	4	5	6	7
$6x$	0	6	4	2	0	6	4	2

So the only solutions are $x \equiv 2 \pmod{8}$ and $x \equiv 6 \pmod{8}$.

Equivalently, the only solution is $x \equiv 2 \pmod{4}$.

Example. Find all solutions to the linear congruence $6x \equiv 4 \pmod{9}$.

Solution. Checking the multiples of 6 while working modulo 9, we have:

x	0	1	2	3	4	5	6	7	8
$6x$	0	6	3	0	6	3	0	6	3

So there are no solutions to $6x \equiv 4 \pmod{9}$.

Linear congruences – Using rules of modular arithmetic

Example. Find all solutions to the linear congruence $6x \equiv 4 \pmod{7}$.

Solution. We have

$$\begin{aligned}6x &\equiv 4 \pmod{7}, \\-x &\equiv 4 \pmod{7}, \\x &\equiv -4 \pmod{7}, \\x &\equiv 3 \pmod{7}.\end{aligned}$$

Example. Find all solutions to the linear congruence $6x \equiv 4 \pmod{8}$.

Solution. We have

$$\begin{aligned}6x &\equiv 4 \pmod{8}, \\3x &\equiv 2 \pmod{4} \quad (\text{since } 2 \mid 8), \\3x &\equiv 6 \pmod{4}, \\x &\equiv 2 \pmod{4} \quad (\text{since } \gcd(3, 4) = 1).\end{aligned}$$

Example. Find all solutions to the linear congruence $6x \equiv 4 \pmod{9}$.

Solution. We must have $6x = 4 + 9k$ for some integer k . But this means $4 = 6x - 9k = 3(2x - 3k)$ where $2x - 3k \in \mathbb{Z}$, which cannot ever be true since $3 \nmid 4$. So there are no solutions.

Solving linear congruences

To solve the general linear congruence $ax \equiv c \pmod{m}$, first consider simplifying the problem using the standard rules of modular arithmetic.

If the coefficient and/or modulus are too large for this to be practical, we can always follow the below method, inspired by the method of finding integer solutions to $ax + my = c$:

- Find $d = \gcd(a, m)$. If $d \nmid c$, there is **no solution**.
- If $d \mid c$, then solutions exist, and there are **exactly d solutions** in the original modulus m . To find these solutions:
 - Find integers x' and y' satisfying $ax' + my' = d$ by applying the **Euclidean algorithm** to a and m and **working backwards**.
 - The general solution is then $x \equiv \frac{c}{d}x' \pmod{\frac{m}{d}}$.
 - If $d > 1$ and we wish to find all d solutions in the **original modulus m** , take the solution $\frac{c}{d}x'$ and **repeatedly add $\frac{m}{d}$** to it until there are d different solutions. That is,

$$x \equiv \frac{c}{d}x' + \frac{m}{d}k \pmod{m}$$

for each $k \in \{0, 1, 2, \dots, d-1\}$.

Solving linear congruences – Example 1

Example. Solve $29x \equiv 11 \pmod{101}$.

Solution. First apply the Euclidean algorithm to the coefficient 29 and the modulus 101. We have

$$101 = 3 \times 29 + 14,$$

$$29 = 2 \times 14 + 1,$$

$$14 = 14 \times 1 + 0.$$

So $\gcd(29, 101) = 1$. Since $1 \mid 11$, there are solutions to the congruence, and there should be exactly 1 solution modulo 101.

Working backwards, we find

$$\begin{aligned} 1 &= 29 - 2 \times 14 \\ &= 29 - 2(101 - 3 \times 29) \\ &= 7 \times 29 - 2 \times 101. \end{aligned}$$

So an integer solution to $29x' + 101y' = 1$ is $x' = 7$ and $y' = -2$.

Since the right-hand side of the congruence is 11, we need to multiply this answer for x' by $\frac{11}{1} = 11$ (and the modulus remains as $\frac{101}{1} = 101$).

So the general solution is $x \equiv 11 \times 7 \equiv 77 \pmod{101}$.

Solving linear congruences – Example 2

Example. Solve $119x \equiv 27 \pmod{252}$.

Solution. First apply the Euclidean algorithm to the coefficient 119 and the modulus 252. We have

$$252 = 2 \times 119 + 14,$$

$$119 = 8 \times 14 + 7,$$

$$14 = 2 \times 7 + 0.$$

So $\gcd(119, 252) = 7$. Since $7 \nmid 27$, there cannot be any solutions to this congruence.

To justify this conclusion, notice that we are trying to solve the equation $119x = 27 + 252k$ for some integer k . But this can be rearranged to give $27 = 119x - 252k = 7(17x - 36k)$ where $17x - 36k \in \mathbb{Z}$, which cannot be true since $7 \nmid 27$. So there are no solutions.

Solving linear congruences – Example 3

Example. Solve $130x \equiv 125 \pmod{245}$.

Solution. First apply the Euclidean algorithm to the coefficient 130 and the modulus 245. We have

$$245 = 1 \times 130 + 115,$$

$$130 = 1 \times 115 + 15,$$

$$115 = 7 \times 15 + 10,$$

$$15 = 1 \times 10 + 5,$$

$$10 = 2 \times 5 + 0.$$

So $\gcd(130, 245) = 5$. Since $5 \mid 125$, there are solutions to the congruence, and there should be exactly 5 solutions modulo 245.

Working backwards, we eventually find $5 = 17 \times 130 - 9 \times 245$. So an integer solution to $130x' + 245y' = 5$ is $x' = 17$ and $y' = -9$.

Since the right-hand side of the congruence is 125, we need to multiply this answer for x' by $\frac{125}{5} = 25$ and reduce the answer modulo $\frac{245}{5} = 49$.

So the general solution is $x \equiv 17 \times 25 \equiv 33 \pmod{49}$, or in the original modulus, by adding 49 repeatedly to our answer, we have $x \equiv 33, 82, 131, 180, \text{ or } 229 \pmod{245}$.

Solving linear congruences – Example 3

Example. Solve $130x \equiv 125 \pmod{245}$.

Alternative approach. Observing that $\gcd(130, 245) = 5$ and that $5 \mid 125$, we first divide everything through by 5 to get the equivalent congruence $26x \equiv 25 \pmod{49}$. Applying the Euclidean algorithm to 26 and 49 gives:

$$49 = 1 \times 26 + 23,$$

$$26 = 1 \times 23 + 3,$$

$$23 = 7 \times 3 + 2,$$

$$3 = 1 \times 2 + 1,$$

$$2 = 2 \times 1 + 0.$$

Working backwards, we eventually find $1 = 17 \times 26 - 9 \times 49$.

Multiplying this equation through by 25 gives the equation

$25 = 425 \times 26 - 225 \times 49$. Considering this equation modulo 49 shows that $25 \equiv 425 \times 26 \equiv 33 \times 26 \pmod{49}$.

So the general solution is $x \equiv 33 \pmod{49}$, or in the original modulus, we have $x \equiv 33, 82, 131, 180, \text{ or } 229 \pmod{245}$.

Solving linear congruences – Example 3

Example. Solve $130x \equiv 125 \pmod{245}$.

Alternative solution. We have

$$130x \equiv 125 \pmod{245},$$

$$26x \equiv 25 \pmod{49} \quad (\text{since } 5 \mid 245),$$

$$75x \equiv 25 \pmod{49},$$

$$3x \equiv 1 \pmod{49} \quad (\text{since } \gcd(25, 49) = 1),$$

$$3x \equiv -48 \pmod{49},$$

$$x \equiv -16 \pmod{49} \quad (\text{since } \gcd(3, 49) = 1),$$

$$x \equiv 33 \pmod{49}.$$

So the general solution is $x \equiv 33 \pmod{49}$, or in the original modulus, we have $x \equiv 33, 82, 131, 180, \text{ or } 229 \pmod{245}$.

Note that this method is much more efficient, but is reliant on finding useful substitutions and is not guaranteed to work efficiently in general.

Multiplicative inverses

Definition. The (multiplicative) inverse of an integer x modulo m (if it exists) is the integer y for which $0 \leq y < m$ and $xy \equiv 1 \pmod{m}$.

Notation. If it exists, we write the inverse of x modulo m as $x^{-1} \pmod{m}$.

For example, the multiplicative inverse of 3 modulo 7 is 5, since $3 \times 5 = 15 \equiv 1 \pmod{7}$. So $3^{-1} \equiv 5 \pmod{7}$. Similarly, we can find:

x	0	1	2	3	4	5	6
$x^{-1} \pmod{7}$	none	1	4	5	2	3	6

Example. Find the multiplicative inverse of 26 modulo 49.

Solution. We want to solve $26x \equiv 1 \pmod{49}$. From the previous example, we saw via the (reversed) Euclidean algorithm that $1 = 17 \times 26 - 9 \times 49$, so $26 \times 17 \equiv 1 \pmod{49}$, meaning that $26^{-1} \equiv 17 \pmod{49}$.

When given the general linear congruence $ax \equiv c \pmod{m}$, if the multiplicative inverse of a exists, we can multiply both sides of the congruence by this value a^{-1} , giving $x \equiv a^{-1}c \pmod{m}$.

If the multiplicative inverse of a does not exist, either there is no solution to the congruence, or $\gcd(a, m) \mid c$, in which case dividing the whole congruence through by $\gcd(a, m)$ will produce a new congruence that we can solve by repeating the above approach.



UNSW
SYDNEY

MATH1081 – Discrete Mathematics

Topic 2 – Number theory and relations

Lecture 2.05 – Relations and equivalences

Lecturer: Dr Sean Gardiner – sean.gardiner@unsw.edu.au

Relations

Definition. Given sets X and Y , a **relation** from X to Y is a subset of $X \times Y$.

Notation. A relation R from a set X to a set Y is declared as $R \subseteq X \times Y$. If $(x, y) \in R$, we can say “ x is related to y ”. Instead of writing $(x, y) \in R$, we can also write $x R y$. If $(x, y) \notin R$, we can write $x \not R y$.

A function is a relation with the additional condition that each element of x has exactly one corresponding y value. That is, $R \subseteq X \times Y$ is a function if and only if for every $x \in X$, there is exactly one $y \in Y$ such that $x R y$.

Notation. Relations can be represented by capital letters like R , but also by symbols like \sim or \preceq . In fact, we have already encountered many relations including $=$, $<$, \leq , \in , \subseteq , and $|$.

For example, the **divisibility relation** $R \subseteq \mathbb{Z} \times \mathbb{Z}$ is defined by the statement

$$a R b \text{ if and only if } b = ak \text{ for some } k \in \mathbb{Z}.$$

So we have $R = \{(0, 0), (1, 0), (1, 1), (1, 2), \dots, (2, 0), (2, 2), (2, 4), \dots\}$.

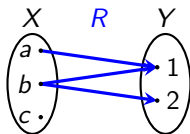
Equivalently, we could just define the divisibility relation $|$ on \mathbb{Z} by

$$a | b \text{ if and only if } b = ak \text{ for some } k \in \mathbb{Z}.$$

Representations of relations

Just like for functions, we can represent relations using **arrow diagrams**.

For example, in the case with sets $X = \{a, b, c\}$ and $Y = \{1, 2\}$, and relation $R \subseteq X \times Y$ given by $R = \{(a, 1), (b, 1), (b, 2)\}$, the relation R can be represented with an arrow diagram as follows:



Note we no longer require each element of X has exactly one outgoing arrow.

We can also represent relations using a **relation matrix**. For a relation from X to Y , we can construct a matrix whose rows are indexed by elements of X and whose columns are indexed by elements of Y such that each matrix entry is either 1 if its corresponding row element is related to its corresponding column element, or 0 otherwise. Note that the appearance of a relation matrix is dependent on the chosen order of rows and columns.

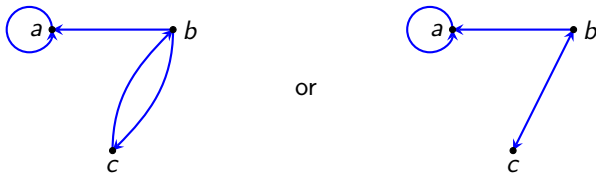
Using the above example, a relation matrix for R is
$$\begin{pmatrix} 1 & 0 \\ 1 & 1 \\ 0 & 0 \end{pmatrix}.$$

Arrow diagrams as directed graphs

Most of the time, we are interested in relations from a set to itself. We refer to a relation $R \subseteq X \times X$ for some set X as a relation on X .

To represent a relation R on X , we can write out the elements of X just once and represent the relation as arrows pointing between these elements. Recall this is known as a **directed graph**, which will appear again in Topic 5.

For example, in the case with set $X = \{a, b, c\}$ and relation R on X given by $R = \{(a, a), (b, a), (b, c), (c, b)\}$, the relation R can be represented with a directed graph arrow diagram as follows:



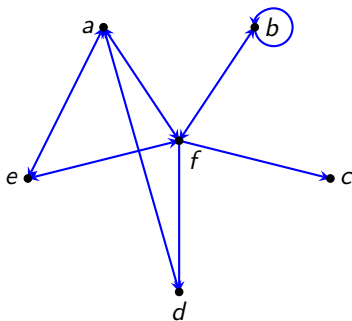
Notice that if two elements are related to each other, we can draw two separate arrows representing these two relations, or just one arrow pointing in both directions.

Example – Representing relations

Example. Consider the set of people $S = \{a, b, c, d, e, f\}$ representing students Alyx, Barney, Chell, Dog, Eli, and Freeman. The relation R on the set S is defined by $x R y$ if and only if x considers y to be their friend. Alyx's friends are Dog, Eli, and Freeman. Barney's friends are Freeman and himself. Dog's friend is Alyx. Eli's friends are Alyx and Freeman. Freeman is friends with everyone else. Represent this relation by a relation matrix and an arrow diagram.

Solution. A relation matrix and arrow diagram for R are provided below.

$$\begin{pmatrix} 0 & 0 & 0 & 1 & 1 & 1 \\ 0 & 1 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 & 0 & 0 \\ 1 & 0 & 0 & 0 & 0 & 0 \\ 1 & 0 & 0 & 0 & 0 & 1 \\ 1 & 1 & 1 & 1 & 1 & 0 \end{pmatrix}$$



Reflexivity

Definition. A relation R on a set X is **reflexive** if and only if for all $x \in X$, we have $x R x$.

In an arrow diagram, a **loop** is an arrow pointing from one element to itself. In terms of arrow diagrams, a relation R is reflexive if and only if **every element has a loop**.

Diagrammatically, this property can be represented as:



Example. Which of the following relations on $X = \{1, 2, 3, 4\}$ are reflexive?

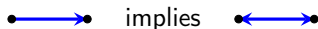
- $R = \{(1, 1), (1, 3), (2, 2), (3, 1), (3, 3), (4, 4)\}$ **is** reflexive since for every element $x \in X$, we have $x R x$.
- $R = \{(1, 1), (1, 3), (2, 4), (3, 1), (3, 3), (4, 2), (4, 4)\}$ is **not** reflexive since for the element $2 \in X$, we do not have $2 R 2$.
- $R = \{(1, 1), (2, 2), (3, 3)\}$ is **not** reflexive since for the element $4 \in X$, we do not have $4 R 4$.

Symmetry

Definition. A relation R on a set X is **symmetric** if and only if for all $x, y \in X$, whenever $x R y$ we have $y R x$.

In terms of arrow diagrams, a relation R is symmetric if and only if **every non-loop arrow points in both directions**.

Diagrammatically, this property can be represented as:



Example. Which of the following relations on $X = \{1, 2, 3, 4\}$ are symmetric?

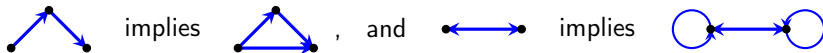
- $R = \{(1, 1), (1, 3), (2, 2), (3, 1), (3, 3), (4, 4)\}$ **is** symmetric since for every pair of elements $x, y \in X$, whenever $x R y$, we have that $y R x$.
- $R = \{(1, 1), (1, 3), (2, 4), (3, 1), (3, 3), (4, 4)\}$ is **not** symmetric since for the elements $2, 4 \in X$, we have $2 R 4$ but $4 \not R 2$.
- $R = \{(1, 1), (2, 2), (3, 3)\}$ **is** symmetric since for every pair of elements $x, y \in X$, whenever $x R y$, we have that $y R x$.
- $R = \{\}$ **is** symmetric since the symmetry condition is satisfied **vacuously**.

Transitivity

Definition. A relation R on a set X is **transitive** if and only if for all $x, y, z \in X$, whenever $x R y$ and $y R z$, we have $x R z$.

In terms of arrow diagrams, a relation R is transitive if and only if **every pair of points connected by a path of arrows also has a single arrow from the first point to the last**.

Diagrammatically, this property can be represented as:



Example. Which of the following relations on $X = \{1, 2, 3, 4\}$ are transitive?

- $R = \{(1, 1), (1, 2), (1, 3), (2, 3), (3, 3), (4, 4)\}$ is transitive since for all elements $x, y, z \in X$, whenever $x R y$ and $y R z$, we have that $x R z$.
- $R = \{(1, 2), (2, 3), (3, 4), (4, 1)\}$ is **not** transitive since for the elements $1, 2, 3 \in X$, we have $1 R 2$ and $2 R 3$ but $1 \not R 3$.
- $R = \{(1, 1), (1, 3), (2, 2), (3, 1), (4, 4)\}$ is **not** transitive since for the elements $1, 3 \in X$, we have $3 R 1$ and $1 R 3$ but $3 \not R 3$.
- $R = \{\}$ is transitive since the transitivity condition is satisfied **vacuously**.

Equivalence relations

Definition. A relation R on a set X is an **equivalence relation** if and only if it is **reflexive**, **symmetric**, and **transitive**.

If two mathematical objects are related by an equivalence relation, we can interpret this as meaning they are **the same** in some particular sense.

For example, a very familiar equivalence relation is $=$ itself. We can easily check that $=$ on any appropriate set is reflexive, symmetric, and transitive.

Example. Show that the relation \sim on \mathbb{Z} defined by setting $x \sim y$ if and only if $x \equiv y \pmod{3}$ is an equivalence relation.

Solution. We proceed by proving \sim is reflexive, symmetric, and transitive.

Reflexivity: Let $x \in \mathbb{Z}$. Since $x = x + 3 \times 0$ and $0 \in \mathbb{Z}$, we can write that $x \equiv x \pmod{3}$. So $x \sim x$, and thus \sim is reflexive.

Symmetry: Let $x, y \in \mathbb{Z}$, and suppose $x \sim y$. Then $x = y + 3k$ for some integer k . So $y = x + 3(-k)$ where $-k \in \mathbb{Z}$, which means $y \equiv x \pmod{3}$. So $y \sim x$, and thus \sim is symmetric.

Transitivity: Let $x, y, z \in \mathbb{Z}$, and suppose $x \sim y$ and $y \sim z$. Then $x = y + 3k$ and $y = z + 3l$ for some integers k and l . So $x = z + 3(l + k)$ where $l + k \in \mathbb{Z}$, which means $x \equiv z \pmod{3}$. So $x \sim z$, and thus \sim is transitive.

Equivalence classes

Definition. Given an equivalence relation \sim on a set X , and some element $a \in X$, the **equivalence class** of a with respect to \sim , written as $[a]$, is the set of all elements in X that are related to a . That is,

$$[a] = \{x \in X : x \sim a\}.$$

For example, if \sim is the equivalence relation on \mathbb{Z} defined by setting $x \sim y$ if and only if $x \equiv y \pmod{2}$, then the equivalence class of 0 with respect to \sim is the set of all integers that have remainder 0 when divided by 2, that is, $[0] = \{\text{even numbers}\}$. Similarly, we have $[1] = \{\text{odd numbers}\}$. Notice that we could also write $[2k] = [0]$ and $[2k + 1] = [1]$ for any integer k .

Indeed, whenever we write $a \equiv b \pmod{m}$, we are really saying $[a] = [b]$ where the equivalence classes are with respect to “**congruence modulo m** ”.

Example. For each of the following equivalence relations \sim on \mathbb{Z} , find the equivalence class of 6.

- Given $x \sim y$ if and only if $x = y$, we have $[6] = \{6\}$.
- Given $x \sim y$ if and only if $x \equiv y \pmod{3}$, we have $[6] = \{3k : k \in \mathbb{Z}\}$.
- Given $x \sim y$ if and only if x has the same number of letters as y when spelled out in English, we have $[6] = \{1, 2, 6, 10\}$.

Properties of equivalence classes

Lemma. Given an equivalence relation \sim on a set X , for all $x \in X$ we have that $x \in [x]$.

Proof. Since \sim is reflexive, we know $x \sim x$ for all $x \in X$. Thus $x \in [x]$.

Lemma. Given an equivalence relation \sim on a set X , for all $x, y \in X$, whenever $x \sim y$ we have $[x] = [y]$.

Proof. For all $a \in [x]$, we have $a \sim x$, and since $x \sim y$, by the transitive property of \sim we have $a \sim y$. So $a \in [y]$, implying $[x] \subseteq [y]$. Next, for all $a \in [y]$, we have $a \sim y$, and since $x \sim y$, by the symmetric property of \sim we have $y \sim x$. So by the transitive property of \sim , we have $a \sim x$. So $a \in [x]$, implying $[y] \subseteq [x]$. Thus $[x] = [y]$.

Theorem. Given an equivalence relation \sim on a set X , the equivalence classes with respect to \sim partition X .

Proof. Clearly the union of all the equivalence classes equals X , since every element $x \in X$ is an element of its own equivalence class $[x]$ (by the first lemma). It remains to show that the different equivalence classes are pairwise disjoint. Suppose we have some $x, y \in X$ such that $[x] \cap [y] \neq \emptyset$. Then there is some $a \in X$ such that $a \in [x]$ and $a \in [y]$. So $a \sim x$ and $a \sim y$, meaning $[a] = [x]$ and $[a] = [y]$ by the second lemma, and so $[x] = [y]$. Thus any pair of non-equal equivalence classes must be disjoint.



UNSW
SYDNEY

MATH1081 – Discrete Mathematics

Topic 2 – Number theory and relations

Lecture 2.06 – Partial orders


Lecturer: Dr Sean Gardiner – sean.gardiner@unsw.edu.au

Antisymmetry

Definition. A relation R on a set X is **antisymmetric** if and only if for all $x, y \in X$, whenever $x R y$ and $y R x$, we have $x = y$.

In terms of arrow diagrams, a relation R is antisymmetric if and only if **it contains no arrows pointing in both directions**.

Diagrammatically, this property can be represented as:

- implies we do **not** have 

Example. Let $X = \{1, 2, 3, 4\}$. Which of the following relations on X are antisymmetric?

- $R = \{(1, 1), (1, 3), (2, 2), (2, 3), (3, 3), (4, 4)\}$ **is** antisymmetric since for every pair of elements $x, y \in X$, whenever $x R y$ and $y R x$, we have that $x = y$.
- $R = \{(1, 1), (1, 3), (2, 4), (3, 1), (3, 3), (4, 2), (4, 4)\}$ **is not** antisymmetric since for the pair of elements $1, 3 \in X$, we have both $1 R 3$ and $3 R 1$, but $1 \neq 3$.

Notice that symmetry and antisymmetry are **not** opposite properties! A given relation can be either, neither, or both symmetric and antisymmetric.

Partial order relations

Definition. A relation R on a set X is a **partial order relation** if and only if it is **reflexive**, **antisymmetric**, and **transitive**.

Definition. If two mathematical objects are related by a partial order relation, we say they are **comparable**. If \preceq is a partial order relation and $x \preceq y$, we can say “ x **precedes** y ” or “ y **succeeds** x ”.

For example, a very familiar partial order relation is \leq on any subset of \mathbb{R} . We can easily check that \leq on \mathbb{R} is reflexive, antisymmetric, and transitive.

Definition. If a relation \preceq is a partial order relation on a set X , we call X a **partially ordered set** or **poset**. We sometimes write a partially ordered set as an ordered pair containing the set and the relation, for example (X, \preceq) .

Definition. If a partially ordered set has the property that all of its elements are comparable with each other, it is called a **totally ordered set**.

For example, (\mathbb{R}, \leq) is a totally ordered set.

Examples of partial order relations

Example. Let S be a set. Show that the relation \preceq on $\mathcal{P}(S)$ defined by setting $X \preceq Y$ if and only if $X \subseteq Y$ is a partial order relation.

Solution. We proceed by proving \preceq is reflexive, antisymmetric, and transitive.

Reflexivity: Let $X \in \mathcal{P}(S)$. Since every element of X is of course an element of X , we know $X \subseteq X$, so $X \preceq X$ and thus \preceq is reflexive.

Antisymmetry: Let $X, Y \in \mathcal{P}(S)$, and suppose $X \preceq Y$ and $Y \preceq X$. Then $X \subseteq Y$ and $Y \subseteq X$, so by definition, we have $X = Y$. Thus \preceq is antisymmetric.

Transitivity: Let $X, Y, Z \in \mathcal{P}(S)$, and suppose $X \preceq Y$ and $Y \preceq Z$. Then $X \subseteq Y$ and $Y \subseteq Z$, so for all $x \in X$ we have $x \in Y$ since $X \subseteq Y$, and therefore $x \in Z$ since $Y \subseteq Z$. So $X \subseteq Z$, meaning $X \preceq Z$, and thus \preceq is transitive.

Hence \preceq acting on $\mathcal{P}(S)$ is a partial order relation.

Examples of partial order relations

Example. Show that the relation \preceq on \mathbb{N} defined by setting $x \preceq y$ if and only if $x \mid y$ is a partial order relation.

Solution. We proceed by proving \preceq is reflexive, antisymmetric, and transitive.

Reflexivity: Let $x \in \mathbb{N}$. Since $x = x \times 1$ and $1 \in \mathbb{Z}$, we can write that $x \mid x$. So $x \preceq x$, and thus \preceq is reflexive.

Antisymmetry: Let $x, y \in \mathbb{N}$, and suppose $x \preceq y$ and $y \preceq x$. Then $y = xk$ and $x = yl$ for some natural numbers k and l . So $x = (xk)l$, implying $kl = 1$, whose only solution over the natural numbers is $k = l = 1$. So $x = y$, and thus \preceq is antisymmetric.

Transitivity: Let $x, y, z \in \mathbb{N}$, and suppose $x \preceq y$ and $y \preceq z$. Then $y = xk$ and $z = yl$ for some natural numbers k and l . So $z = (xk)l$ where $kl \in \mathbb{N}$, which means $x \mid z$. So $x \preceq z$, and thus \preceq is transitive.

Hence \preceq acting on \mathbb{N} is a partial order relation.

Notice that if this relation \preceq acted on the set \mathbb{Z} instead of \mathbb{N} , the relation would no longer be antisymmetric and therefore (\mathbb{Z}, \mid) would **not** be a partially ordered set. (For example, $1 \mid -1$ and $-1 \mid 1$ but $1 \neq -1$.)

Hasse diagrams

Notation. Given \preceq is a partial order relation on some set X , we use the symbol \prec to mean “precedes but does not equal”. That is, $x \prec y$ means $x \preceq y$ and $x \neq y$.

Definition. A **Hasse diagram** is a simplified way of representing a partially ordered set. Given a partial order relation \preceq on a set X , the Hasse diagram for the partially ordered set (X, \preceq) is constructed as follows:

- Draw a labelled dot for each element of X .
- For each pair of elements $x, y \in X$, draw a line from x to y with x placed **lower** than y if and only if both
 - $x \prec y$, and
 - there does **not** exist $z \in X$ such that $x \prec z$ and $z \prec y$.

A Hasse diagram contains all the information of a usual arrow diagram for a poset, but in a simpler format.

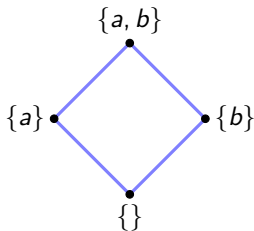
- Arrowheads are not needed since direction is implied by element position.
- Loops are not included since they must exist at every element.
- Lines implied by transitivity are not included since they must exist for every upward path.

Hasse diagrams – subset example

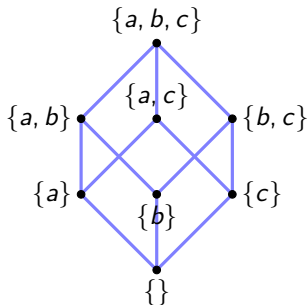
Example. Draw the Hasse diagram for the partially ordered sets $(\mathcal{P}(\{a, b\}), \subseteq)$ and $(\mathcal{P}(\{a, b, c\}), \subseteq)$.

Solution.

The Hasse diagram for the poset $(\mathcal{P}(\{a, b\}), \subseteq)$ is:



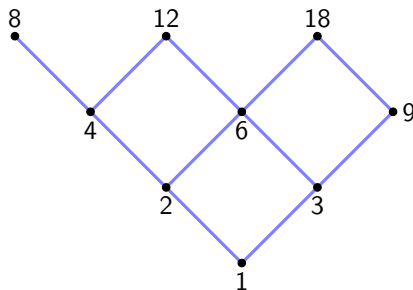
The Hasse diagram for the poset $(\mathcal{P}(\{a, b, c\}), \subseteq)$ is:



Hasse diagrams – divisibility example

Example. Draw the Hasse diagram for the partially ordered set $(\{1, 2, 3, 4, 6, 8, 9, 12, 18\}, |)$.

Solution. The Hasse diagram for the poset $(\{1, 2, 3, 4, 6, 8, 9, 12, 18\}, |)$ is:



Least and greatest elements

Definition. A **minimal element** of a partially ordered set (X, \preceq) is any element $x \in X$ such that there is **no** $y \in X$ where $y \prec x$.

In terms of Hasse diagrams, a minimal element is an element with no lines connecting to it **from below**.

Definition. A **maximal element** of a partially ordered set (X, \preceq) is any element $x \in X$ such that there is **no** $y \in X$ where $x \prec y$.

In terms of Hasse diagrams, a maximal element is an element with no lines connecting to it **from above**.

Definition. The **least element** of a partially ordered set (X, \preceq) (if it exists) is the element $x \in X$ for which $x \preceq y$ for all $y \in X$.

In terms of Hasse diagrams, the least element is the element that can reach all other elements in X by following lines in a strictly **upwards** path.

Definition. The **greatest element** of a partially ordered set (X, \preceq) (if it exists) is the element $x \in X$ for which $y \preceq x$ for all $y \in X$.

In terms of Hasse diagrams, the greatest element is the element that can reach all other elements in X by following lines in a strictly **downwards** path.

Least and greatest elements – Examples and properties

Example. Find the minimal, maximal, least, and greatest elements of $(\mathcal{P}(\{a, b, c\}), \subseteq)$.

Solution. The only minimal element is $\{\}$, which is also the least element. The only maximal element is $\{a, b, c\}$, which is also the greatest element.

Example. Find the minimal, maximal, least, and greatest elements of $(\{1, 2, 3, 4, 6, 8, 9, 12, 18\}, |)$.

Solution. The only minimal element is 1, which is also the least element. The maximal elements are 8, 12, and 18. There is no greatest element, since for example, 8 and 12 are not comparable.

Fact. The following statements are true for any partially ordered set (X, \preceq) .

- If it exists, the least element is **unique**.
- If it exists, the greatest element is **unique**.
- If X is **finite**, the poset has a least element if and only if it has **exactly one** minimal element.
- If X is **finite**, the poset has a greatest element if and only if it has **exactly one** maximal element.

Lower and upper bounds

Definition. Given a partially ordered set (X, \preceq) , a **lower bound** of two elements $x, y \in X$ is any element $z \in X$ such that $z \preceq x$ and $z \preceq y$.

In terms of Hasse diagrams, a lower bound of x and y is any element that can reach both x and y by following lines in strictly **upwards** paths.

Definition. Given a partially ordered set (X, \preceq) , the **greatest lower bound** of two elements $x, y \in X$, denoted $\text{glb}(x, y)$, is the greatest element amongst the set of all lower bounds (if it exists). That is, $\text{glb}(x, y)$ is the greatest element (if it exists) of $\{z \in X : z \preceq x \text{ and } z \preceq y\}$.

Definition. Given a partially ordered set (X, \preceq) , an **upper bound** of two elements $x, y \in X$ is any element $z \in X$ such that $x \preceq z$ and $y \preceq z$.

In terms of Hasse diagrams, an upper bound of x and y is any element that can reach both x and y by following lines in strictly **downwards** paths.

Definition. Given a partially ordered set (X, \preceq) , the **least upper bound** of two elements $x, y \in X$, denoted $\text{lub}(x, y)$, is the least element amongst the set of all upper bounds (if it exists). That is, $\text{lub}(x, y)$ is the least element (if it exists) of $\{z \in X : x \preceq z \text{ and } y \preceq z\}$.

Lower and upper bounds – Examples and properties

Example. In the poset $(\mathcal{P}(\{a, b, c\}), \subseteq)$, find $\text{glb}(\{a, b\}, \{b, c\})$ and $\text{lub}(\{a\}, \{a, b\})$ if they exist.

Solution. The lower bounds of $\{a, b\}$ and $\{b, c\}$ are $\{b\}$ and $\{\}$, so the greatest lower bound exists and is $\{b\}$. The upper bounds of $\{a\}$ and $\{a, b\}$ are $\{a, b\}$ and $\{a, b, c\}$, so the least upper bound exists and is $\{a, b\}$.

Example. In the poset $(\{1, 2, 3, 4, 6, 8, 9, 12, 18\}, |)$, find $\text{glb}(12, 18)$ and $\text{lub}(4, 9)$ if they exist.

Solution. The lower bounds of 12 and 18 are 1, 2, 3, and 6, so the greatest lower bound exists and is 6. There is no upper bound for 4 and 9, so their least upper bound does not exist in this poset.

Fact. For any set S , in the partially ordered set $(\mathcal{P}(S), \subseteq)$, for any two elements $A, B \in \mathcal{P}(S)$ we have $\text{glb}(A, B) = A \cap B$ and $\text{lub}(A, B) = A \cup B$.

Fact. In the partially ordered set $(\mathbb{Z}^+, |)$, for any two elements $a, b \in \mathbb{Z}^+$ we have $\text{glb}(a, b) = \text{gcd}(a, b)$ and $\text{lub}(a, b) = \text{lcm}(a, b)$.

Note that the least element of $(\mathbb{Z}^+, |)$ is 1, but it has no greatest element. If we use the “alternate definition” given for the GCD and LCM, the above facts also hold for the poset $(\mathbb{N}, |)$, whose greatest element is 0.