

§2 Integers, Modular Arithmetic, and Relations

FACTORISATION

- We recall the commonly-used sets in our number system:
 - *Positive integers* $\mathbb{Z}^+ = \{1, 2, 3, \dots\}$.
 - *Natural numbers* $\mathbb{N} = \{0, 1, 2, 3, \dots\}$.
 - *Integers* $\mathbb{Z} = \{\dots, -2, -1, 0, 1, 2, \dots\}$.
 - *Rational numbers* $\mathbb{Q} = \{\frac{p}{q} \mid p, q \in \mathbb{Z}, q \neq 0\}$.
 - *Real numbers* \mathbb{R} (includes \mathbb{Q} and *irrational numbers* such as $\sqrt{2}$, π , e).
- Note that $\mathbb{Z}^+ \subseteq \mathbb{N} \subseteq \mathbb{Z} \subseteq \mathbb{Q} \subseteq \mathbb{R}$.
- *Number theory* focuses on \mathbb{Z} and its subsets.
- We can add, multiply, subtract, and divide in \mathbb{Q} and \mathbb{R} , but we cannot always divide in \mathbb{Z} ; for instance, $\frac{2}{3} \notin \mathbb{Z}$.

- Let a and b be integers. If there is an integer m such that $b = am$, then we say
 - b is a *multiple* of a ,
 - a is a *factor* or *divisor* of b ,
 - a *divides* b ,
 - b is *divisible* by a ,
 - am is a *factorisation* of b
 and we write $a \mid b$.
- We write $a \nmid b$ if a does not divide b .
- If a and b are positive integers and $a \mid b$, then we must have $a \leq b$.
- $a \mid b$ (“ a divides b ”) is a statement about *divisibility* that is either true or false.
 $\frac{a}{b}$ (“ a divided by b ”) is a number that we get by carrying out *division*.
 The divisibility symbol $a \mid b$ and the division symbol a/b are not to be confused.
- Divisibility by zero is well-defined but mostly pointless, since $0 \mid b$ only holds when $b = 0$.

Exercise. Compare the following notations.

$$12/48$$

$$\frac{12}{48}$$

$$12 \mid 48$$

$$12 \nmid 48$$

$$48/12$$

$$\frac{48}{12}$$

$$48 \mid 12$$

$$48 \nmid 12$$

● **Properties of divisibility:** let a , b , and c be integers, then

(i) $a \mid 0$, (Each integer is a factor of 0 and 0 is a multiple of every integer.)

(ii) if $a \mid b$, then $a \mid bc$;

(iii) if $a \mid b$ and $a \mid c$, then $a \mid (b + c)$;

(iv) if $a \mid b$ and $a \mid c$, then $a \mid (sb + tc)$ for all integers s and t ; (Important!)

(v) if $a \mid b$ and $b \mid c$, then $a \mid c$. (*Transitivity* of divisibility)

Proof. (v) Suppose that $a \mid b$ and $b \mid c$.

Then $b = am$ and $c = bn$ for some integers m and n . Thus, we have

$$c = bn = (am)n = a(mn) = ak,$$

where $k = mn$ is an integer. Hence, $a \mid c$.

(i) $0 = a \times 0$. Thus, $a \mid 0$.

Exercise. Prove (ii)-(iv).

● Simple divisibility tests:

2	Last digit is 0, 2, 4, 6, or 8.
3	Sum of digits is divisible by 3.
4	Last two digits is divisible by 4.
5	Last digit is 0 or 5.
6	Divisible by 2 and 3.
7	Double the last digit and subtract it from the remaining leading truncated number. If the result is divisible by 7, then so was the original number. Apply this rule over and over again as necessary.
8	Last three digits is divisible by 8.
9	Sum of digits is divisible by 9.
10	Last digit is 0.
11	The difference between the sum of digits in the odd positions and the sum of digits in the even positions is divisible by 11.
⋮	

Exercise.

Is 408254 a multiple of 3? Is 408254 divisible by 7? Does 11 divide 408254?

- An *even* number is an integer that is divisible by 2, so can be written as $n = 2k$ for some integer k .
- An *odd* number is an integer that is not an even number so can be written as $n = 2k + 1$ for some integer k .

- A **prime** is an integer larger than 1 whose only positive factors are 1 and itself.
 - The first few primes are 2, 3, 5, 7, 11, 13, 17, 19, 23, 29, . . .
 - There are infinitely many primes; this has been known for over two thousand years.
 - Primes of the form $2^p - 1$, where p is prime, are called **Mersenne primes**. The largest prime currently known (March 1st 2014) is a Mersenne prime, $2^{57,885,161} - 1$, discovered in January 2013. It has 17,425,170 digits. Check out GIMPS for the latest information.
 - Primes of the form $2^{2^n} + 1$ are known as **Fermat primes**. Only five Fermat primes are known: 3, 5, 17, 257, 65537.
 - **Twin primes** are pairs of primes that differ by 2, such as 3 and 5, 5 and 7, 11 and 13, 17 and 19, and 1000000000061 and 1000000000063. There are thought to be infinitely many twin primes but no proof exists.
- An integer greater than 1 that is not a prime is called a **composite** number.
- 1 is neither prime nor composite.

- **The Fundamental Theorem of Arithmetic.**
Any positive integer n has a prime factorization, that is, can be expressed as a product of primes

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

for distinct primes p_1, p_2, \dots, p_k and exponents $\alpha_1, \alpha_2, \dots, \alpha_k \in \mathbb{Z}^+, k \geq 0$.

- The factorisation is **unique up to permuting factors**.
- A prime number is a product of just one prime, namely itself.
- 1 is a product of no primes.
- Any positive divisor d of the above n has prime factorisation

$$d = p_1^{\beta_1} p_2^{\beta_2} \cdots p_k^{\beta_k},$$

for some $0 \leq \beta_1 \leq \alpha_1, \dots, 0 \leq \beta_k \leq \alpha_k$.

Example.

$$1000 = 2^3 \times 5^3; \quad 1001 = 7 \times 11 \times 13; \quad 1002 = 2 \times 3 \times 167.$$

“Algorithm” to find the prime factorisation of n . If n is prime, we are done. Otherwise, we can factorise $n = ab$ with a, b positive factors not equal to 1. Repeat procedure with a and b .

Exercise. Find the prime factorisation of 345 and all its positive factors.

- How do we determine whether or not a given positive integer n is prime?
 - The obvious way to do this is to check whether n is a multiple of any of the $n - 2$ numbers $2, 3, \dots, n - 1$. If none of these is a factor, then n is prime; if any of them is a factor, then n is composite.
 - It is enough to check only the primes among these $n - 2$ numbers. (**Why?**)
 - It is enough to check only the primes up to \sqrt{n} . (See next page.)
 - There are faster primality tests. (See MATH2400 and MATH3411.)

● **Theorem.** If n is composite, then n has a prime factor at most equal to \sqrt{n} .
Equivalently...

● **Theorem.** If n has no prime factor less than or equal to \sqrt{n} , then it is prime.

Proof.

Exercise. Is 161 prime? Is 163 prime?

- Let a and b be integers, not both zero. Any positive integer d that satisfies $d \mid a$ and $d \mid b$ is called a *common divisor* or a *common factor* of a and b . The largest such d is called the *greatest common divisor* of a and b , and is denoted by $\gcd(a, b)$.
- If $\gcd(a, b) = 1$, then a and b are *coprime* or *relatively prime* to each other.
- Let a and b be positive integers. Each positive integer m that satisfies both $a \mid m$ and $b \mid m$ is called a *common multiple* of a and b . The smallest such m is called the *least common multiple* of a and b , and is denoted by $\text{lcm}(a, b)$.
- If a and b are positive integers, then $\gcd(a, b) \times \text{lcm}(a, b) = ab$.

Example. The positive factors of 12 are $\{1, 2, 3, 4, 6, 12\}$.

The positive divisors of 42 are $\{1, 2, 3, 6, 7, 14, 21, 42\}$.

The common divisors of 12 and 42 are $\{1, 2, 3, 6\}$.

Thus, $\gcd(12, 42) = 6$.

The positive multiples of 12 are $\{12, 24, 36, 48, 60, 72, 84, \dots\}$.

The positive multiples of 42 are $\{42, 84, 126, \dots\}$.

Thus, $\text{lcm}(12, 42) = 84$.

Example. Since prime factorisation can be used to find all divisors of an integer, it can also be used to find the gcd and lcm of two numbers. For example, consider

$$14175 = 3^4 \times 5^2 \times 7 \quad \text{and} \quad 16758 = 2 \times 3^2 \times 7^2 \times 19.$$

For the gcd, we multiply all the prime factors common to both:

$$\gcd(14175, 16758) = 3^2 \times 7 = 63.$$

For the lcm, take the smallest product that includes all factors of both numbers:

$$\text{lcm}(14175, 16758) = 2 \times 3^4 \times 5^2 \times 7^2 \times 19 = 3770550.$$

Exercise. Find the gcd and lcm of $a = 2^3 \times 3 \times 5^2 \times 11$ and $b = 3 \times 5 \times 7$.

Exercise. If a is positive and is a factor of b , then what is $\gcd(a, b)$?

Exercise. What happens if we try to compute $\gcd(0, 0)$?

Exercise. What is $d = \gcd(\frac{a}{\gcd(a,b)}, \frac{b}{\gcd(a,b)})$?

EUCLIDEAN ALGORITHM & INTEGER ARITHMETIC

A key tool in integer arithmetic is

● **The Division Algorithm.** Let a be an integer and b be a positive integer. Then there is a unique pair of integers q and r (called *quotient* and *remainder*) such that $a = qb + r$ and $0 \leq r < b$.

Proof. See textbook [Epp, Section 4.4 and Exercise 18 of Section 3.7].

Example. We can find the quotient and remainder by long division or by repeated subtraction. For example, we divide 92 and -92 by 7.

$\begin{array}{r} 13 \\ 7 \overline{)92} \\ \underline{7} \\ 22 \\ \underline{21} \\ 1 \end{array}$	$\begin{array}{r} 13 \\ 7 \overline{)92} \\ \underline{91} \\ 1 \end{array}$	$\begin{array}{r} -13 \\ 7 \overline{)-92} \\ \underline{-91} \\ -1 \end{array}$	$\begin{array}{r} -14 \\ 7 \overline{)-92} \\ \underline{-98} \\ 6 \end{array}$
<i>long division</i>	<i>simplified</i>	<i>incorrect</i>	<i>correct</i>

We see that $92 = 13 \times 7 + 1$.

Thus, when 92 is divided by 7, the quotient is 13 and the remainder 1.

We have $-92 = (-13) \times 7 + (-1)$ and $-92 = (-14) \times 7 + 6$. Since the remainder should lie between 0 and 6, we conclude that when -92 is divided by 7, the quotient is -14 and the remainder 6.

Exercise. Find the quotient and remainder when -1001 is divided by 101.

● **Theorem.** Let a , b , q , and r be integers such that $a = qb + r$, where a and b are not both zero. Then

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

Proof. Write $d_1 = \gcd(a, b)$ and $d_2 = \gcd(b, r)$.

Since $d_2 \mid b$ and $d_2 \mid r$, we have $d_2 \mid (qb + r)$ and thus $d_2 \mid a$.

Thus d_2 is a common divisor of a and b .

But since d_1 is the greatest common divisor of a and b , we must have $d_2 \leq d_1$.

Conversely, we can write $r = a - qb$.

Since $d_1 \mid a$ and $d_1 \mid b$, we have $d_1 \mid (a - qb)$ and thus $d_1 \mid r$.

This shows that d_1 is a common divisor of b and r , and hence $d_1 \leq d_2$.

For both $d_2 \leq d_1$ and $d_1 \leq d_2$ to be true we require that $d_1 = d_2$.

● **Euclidean Algorithm.** Use the above theorem together with the Division Algorithm repeatedly to calculate the greatest common divisor of two numbers.

Note that we underline a, b, r and the successive remainders as we need to keep track of them, particularly later.

Example. We use the Euclidean Algorithm to compute the greatest common divisor of 16758 and 14175 as follows:

$$\begin{aligned}
\underline{16758} &= 1 \times \underline{14175} + \underline{2583}, & \text{so } \gcd(16758, 14175) &= \gcd(14175, 2583). \\
\underline{14175} &= 5 \times \underline{2583} + \underline{1260}, & \text{so } \gcd(14175, 2583) &= \gcd(2583, 1260). \\
\underline{2583} &= 2 \times \underline{1260} + \underline{63}, & \text{so } \gcd(2583, 1260) &= \gcd(1260, 63). \\
\underline{1260} &= 20 \times \underline{63} + 0, & \text{thus } 63 \mid 1260 \text{ and so } \gcd(1260, 63) &= 63.
\end{aligned}$$

Hence, $\gcd(16758, 14175) = 63$. Moreover, we have

$$\text{lcm}(16758, 14175) = \frac{16758 \times 14175}{\gcd(16758, 14175)} = 3770550.$$

Exercise. Use the Euclidean Algorithm to find $\gcd(854, 651)$.

● We can use the Euclidean Algorithm to find an integer solution x and y to the equation

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

This is done by working backward through the Euclidean Algorithm; this process is known as the *Extended Euclidean Algorithm*.

Example. We look for an integer solution of x and y to the equation

$$16758x + 14175y = 63.$$

Recall that we obtained $\gcd(16758, 14175) = 63$ by the Euclidean Algorithm

$$\underline{16758} = 1 \times \underline{14175} + \underline{2583} \tag{3}$$

$$\underline{14175} = 5 \times \underline{2583} + \underline{1260} \tag{2}$$

$$\underline{2583} = 2 \times \underline{1260} + \underline{63} \tag{1}$$

$$\underline{1260} = 20 \times \underline{63} + 0.$$

We work backwards, re-writing the remainders using (1)-(3):

$$\underline{63} = \underline{2583} - 2 \times \underline{1260} \quad \text{by equation (1)}$$

$$\begin{aligned}
&= \underline{2583} - 2(\underline{14175} - 5 \times \underline{2583}) && \text{by equation (2)} \\
&= 11 \times \underline{2583} - 2 \times \underline{14175} && \text{collect like terms} \\
&= 11(\underline{16758} - \underline{14175}) - 2 \times \underline{14175} && \text{by equation (3)} \\
&= 11 \times \underline{16758} - 13 \times \underline{14175} && \text{collect like terms.}
\end{aligned}$$

Thus,

$$16758 \times 11 + 14175 \times (-13) = 63.$$

Hence, $16758x + 14175y = 63$ has an integer solution $x = 11$ and $y = -13$.

• Doubling this equation we see that

$16758x + 14175y = 126$ has an integer solution $x = 22$ and $y = -26$, since

$$16758 \times (11 \times 2) + 14175 \times (-13 \times 2) = 63 \times 2.$$

• Tripling this equation we see that

$16758x + 14175y = 189$ has an integer solution $x = 33$ and $y = -39$, since

$$16758 \times (11 \times 3) + 14175 \times (-13 \times 3) = 63 \times 3.$$

• However, $16758x + 14175y = 60$ has no integer solution, since $63 \nmid 60$ but $63 \mid \text{LHS}$.

Above examples show the extended Euclidean algorithm gives (i) & (ii) below.

• **The Bézout Property.** Consider the equation

$$ax + by = c,$$

where a , b , and c are integers, with a and b not both zero. Then

- (i) if $c = \gcd(a, b)$, then the equation has integer solutions;
- (ii) if $c = e \gcd(a, b)$ for some $e \in \mathbb{Z}$, then the equation has integer solutions;
In fact if $(x, y) = (x_0, y_0)$ is a solution to $ax + by = \gcd(a, b)$ then $(x, y) = (ex_0, ey_0)$ is a solution to $ax + by = e \gcd(a, b)$.
- (iii) if c is not a multiple of $\gcd(a, b)$, then the equation has no integer solution.

Proof of (iii) Let $d = \gcd(a, b)$. Suppose now that c is not a multiple of d and x and y are numbers satisfying $ax + by = c$. If x, y were integers, then we would have $d \mid (ax + by)$ and hence $d \mid c$, which contradicts the fact that c is not a multiple of d . Hence, in this case x and y cannot be integers and (iii) is proved.

Exercise. Use the Extended Euclidean Algorithm to find integer solutions to the equations

$$a) 520x - 1001y = 13, \quad b) 520x - 1001y = -26, \quad \text{and} \quad c) 520x - 1001y = 1.$$

Note that we solve $520x + 1001z = 13$ then put $y = -z$.

MODULAR ARITHMETIC

● Recall that the Division Algorithm states

if a is an integer and m is a positive integer, then there exist unique integers q and r , called the quotient and the remainder, respectively, such that $a = qm + r$ and $0 \leq r < m$.

We define $a \bmod m$ (reads “ a modulo m ”) to be this remainder r .

We essentially “ignore” multiples of the modulus m .

Exercise. Evaluate

$$11 \bmod 3$$

$$5 \bmod 7$$

$$-11 \bmod 3$$

$$-5 \bmod 7$$

● Let m be a positive integer. Two integers a and b are congruent modulo m , denoted by $a \equiv b \pmod{m}$, if

$$(a \bmod m) = (b \bmod m),$$

that is, if a and b have the same remainder when divided by m .

Example. Any two odd numbers are congruent modulo 2.

● **Equivalent definitions of congruence:**

- (i) $a \equiv b \pmod{m}$,
- (ii) $(a \bmod m) = (b \bmod m)$,
- (iii) $m \mid (a - b)$,
- (iv) $a = b + km$ for some integer k .

Proof.

(i) and (ii) are equivalent by definition.

(iii) and (iv) are equivalent by definition.

Let us prove that (ii) implies (iii).

Suppose that $(a \bmod m) = (b \bmod m) = r$ for some integer $0 \leq r < m$.

Then $a = q_1m + r$ and $b = q_2m + r$ for some integers q_1 and q_2 . Thus,

$$a - b = (q_1m + r) - (q_2m + r) = (q_1 - q_2)m = km,$$

where $k = q_1 - q_2$ is an integer. Hence, we have $m \mid (a - b)$.

Finally, let us prove that (iv) implies (ii). (Why does this prove the result?)

● **Properties of congruence:** if $a \equiv b \pmod{m}$ 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) $a^n \equiv b^n \pmod{m}$ for all $n \geq 0$;
- (v) $\ell a \equiv \ell b \pmod{m}$ for all integers ℓ ;
- (vi) $a \equiv b \pmod{n}$ for all integers n satisfying $n \mid m$.

Proof.

Suppose that $a = b + k_1m$ and $c = d + k_2m$ for some integers k_1 and k_2 .

(i) $a + c = (b + k_1m) + (d + k_2m) = (b + d) + (k_1 + k_2)m = (b + d) + km$, where $k = k_1 + k_2$ is an integer. Thus, $a + c \equiv b + c \pmod{m}$.

(ii) Similar to (i).

Example. Suppose $x, y \in \mathbb{Z}$ with $x \equiv 3 \pmod{7}$, $y \equiv 5 \pmod{7}$.

Find $2x + xy \pmod{7}$.

By v), $2x \equiv 2 \times 3 = 6 \pmod{7}$.

By iii), $xy \equiv 3 \times 5 = 15 \equiv 1 \pmod{7}$.

So i) gives $2x + xy \equiv 6 + 1 = 7 \equiv 0 \pmod{7}$. Hence $2x + xy \pmod{7} = 0$.

Exercise. Find $x^3 + 2x^2y \pmod{7}$.

Upshot You can substitute with congruence equations much as you can with ordinary equations.

Here's a simple-minded application of modular arithmetic.

Example. The last two digits of the number 1234567 are the number 67. This can be formally expressed as

$$1234567 \bmod 100 = 67 \quad \text{or} \quad 1234567 \equiv 67 \pmod{100}.$$

Similarly, to find the last two digits of the number $7^{1234567}$, we need to evaluate $7^{1234567} \bmod 100$. We have

$$\begin{aligned} 7^2 &\equiv 49 \pmod{100}; \\ 7^3 &\equiv 49 \times 7 \equiv 343 \equiv 43 \pmod{100}; \\ 7^4 &\equiv 43 \times 7 \equiv 301 \equiv 1 \pmod{100}. \end{aligned}$$

Then it is easy to obtain, for example,

$$\begin{aligned} 7^8 &\equiv (7^4)^2 \equiv 1^2 \equiv 1 \pmod{100}; \\ 7^{444} &\equiv (7^4)^{111} \equiv 1^{111} \equiv 1 \pmod{100}; \\ 7^{446} &\equiv (7^4)^{111} \times 7^2 \equiv 1^{111} \times 49 \equiv 49 \pmod{100}; \end{aligned}$$

and in particular, we have

$$7^{1234567} \equiv 7^{4 \times 308641 + 3} \equiv (7^4)^{308641} \times 7^3 \equiv 1^{308641} \times 43 \equiv 43 \pmod{100}.$$

Exercise. Simplify $10^{123456789} \bmod 41$.

Example. We have seen that simplifying $a^n \bmod m$ becomes quite easy if there is a small number k such that $a^k \equiv 1 \pmod{m}$. In a similar way, it is also useful if we have $a^k \equiv -1 \pmod{m}$ for some small k . The trick is to try and keep the numbers between $-m/2$ and $m/2$.

For example, we will try to simplify $5^{115511} \bmod 29$. We have

$$\begin{aligned} 5^2 &\equiv 25 \equiv -4 \pmod{29}; && \text{usual remainder 25 not used!} \\ 5^3 &\equiv (-4) \times 5 \equiv -20 \equiv 9 \pmod{29}; \\ 5^4 &\equiv 9 \times 5 \equiv 45 \equiv 16 \equiv -13 \pmod{29}; \\ 5^5 &\equiv (-13) \times 5 \equiv -65 \equiv -7 \pmod{29}; \\ 5^6 &\equiv (-7) \times 5 \equiv -35 \equiv -6 \pmod{29}; \\ 5^7 &\equiv (-6) \times 5 \equiv -30 \equiv -1 \pmod{29}. \end{aligned}$$

Thus,

$$\begin{aligned} 5^{115511} &\equiv 5^{7 \times 16501 + 4} \equiv (5^7)^{16501} \times 5^4 \\ &\equiv (-1)^{16501} \times (-13) \equiv (-1) \times (-13) \equiv 13 \pmod{29}. \end{aligned}$$

Example. Unfortunately, we can't find k with $a^k \equiv \pm 1 \pmod{m}$ if $\gcd(a, m) \neq 1$. Instead we keep an eye out for any "pattern" in the numbers.

For example, we now try to simplify $6^{54321} \bmod 100$. We have

$$\begin{aligned} 6^1 &\equiv 6 \pmod{100}; \\ 6^2 &\equiv 36 \pmod{100}; \\ 6^3 &\equiv 36 \times 6 \equiv 216 \equiv 16 \pmod{100}; \\ 6^4 &\equiv 16 \times 6 \equiv 96 \equiv -4 \pmod{100}; \\ 6^5 &\equiv (-4) \times 6 \equiv -24 \pmod{100}; \\ 6^6 &\equiv (-24) \times 6 \equiv -144 \equiv -44 \pmod{100}; \\ 6^7 &\equiv (-44) \times 6 \equiv -264 \equiv 36 \pmod{100}. \end{aligned}$$

Since $6^7 \equiv 6^2 \pmod{100}$, the numbers repeat every 5 steps from here on. Thus,

$$6^{54321} \equiv 6^{54316} \equiv 6^{54311} \equiv \dots \equiv 6^6 \equiv -44 \equiv 56 \pmod{100}.$$

Since $6^6 \not\equiv 6^1 \pmod{100}$, the pattern does *not* hold for smaller powers. The pigeon-hole principle (topic 4) ensures there will eventually be a pattern.

Exercise. A notice at the bus stop says that

“Buses depart at x minutes past the hour, where $x \equiv 7 \pmod{15}$ ”.

Thus $x \equiv 7, 22, 37, 52 \pmod{60}$.

In usual parlance, we say buses leave at 7, 22, 37, 52 minutes past the hour.

Recall that **real** numbers a, b are *inverses* if $ab = 1$.

● Let m be a positive integer and $a, b \in \mathbb{Z}$ be such that $ab \equiv 1 \pmod{m}$.

Then we say

● a, b are *inverses* modulo m .

● b is an *inverse* of a modulo m .

● In this case, for any integer k ,

$$a(b + km) \equiv ab \equiv 1 \pmod{m}$$

so $b + km$ is also an inverse of a modulo m .

Example. 3, 4 are inverses modulo 11 since $3 \times 4 = 12 \equiv 1 \pmod{11}$.

Example. Use the extended Euclidean algorithm to find an inverse x of 40 modulo 77.

1. We re-write the congruence equation $40x \equiv 1 \pmod{77}$ as the ordinary equation

$$40x - 1 = 77y, \quad \text{for some } y \in \mathbb{Z}.$$

This is equivalent to $40x - 77y = 1$.

N.B. $\gcd(40, 77) = 1$ so there is a solution.

2. We now use the extended Euclidean algorithm to find x .

$$\underline{77} = 1 \times \underline{40} + \underline{37}$$

$$\underline{40} = 1 \times \underline{37} + \underline{3}$$

$$\underline{37} = 12 \times \underline{3} + \underline{1}$$

$$\underline{3} = 3 \times \underline{1} + 0$$

$$\underline{1} = \underline{37} - 12 \times \underline{3}$$

$$= \underline{37} - 12(\underline{40} - \underline{37})$$

$$= 13 \times \underline{37} - 12 \times \underline{40}$$

$$= 13(\underline{77} - \underline{40}) - 12 \times \underline{40}$$

$$= 13 \times \underline{77} - 25 \times \underline{40}$$

Thus, $40 \times (-25) - 77 \times (-13) = 1$.

This gives a solution $x = -25$ (we don't care about y).

This shows that we have the following inverses of 40 modulo 77

$x = \dots, -25, -25 + 77, -25 + 2 \times 77, \dots = \dots, -25, 52, 129, \dots$

Exercise. Find an inverse n of 5 modulo 11.

● **Typical Question.** Given integers a, b and a positive integer m , find all integers x satisfying the condition

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

This is a problem of *solving a linear congruence*.

There are several cases to consider in solving this congruence equation.

● **Theorem.** If $\gcd(a, m)$ is not a factor of b , then the congruence $ax \equiv b \pmod{m}$ has no (integer) solutions.

Proof. The congruence equation requires solving $ax + my = b$ for some integers x, y . But we know there are no solutions unless $\gcd(a, m) | b$.

Example. Does $6x \equiv 3 \pmod{8}$ have solutions?

Answer: No, because $\gcd(6, 8) = 2$ and $2 \nmid 3$.

The next case is $\gcd(a, m) = 1$ so automatically $\gcd(a, m) | b$.

● **Theorem.** Suppose $\gcd(a, m) = 1$ and let c be an inverse of a modulo m . Then the solution to $ax \equiv b \pmod{m}$ is any integer x such that $x \equiv cb \pmod{m}$.

Proof. Suppose first that x is a solution to $ax \equiv b \pmod{m}$. Multiplying both sides of the congruence equation by c shows that

$$cb \equiv cax \equiv 1x \equiv x \pmod{m}.$$

Conversely, if $x \equiv cb \pmod{m}$ then

$$ax \equiv acb \equiv 1b \equiv b \pmod{m}.$$

Example. We want to find all (integer) solutions to

$$79x \equiv 12 \pmod{45}.$$

1. Note that $\gcd(79, 45) = 1$, so the theorem suggests we should find an inverse c of 79 modulo 45.
2. As before, we find c using the Extended Euclidean Algorithm:

$$\begin{array}{ll} \underline{79} = 1 \times \underline{45} + \underline{34} & \underline{1} = \underline{34} - 3 \times \underline{11} \\ \underline{45} = 1 \times \underline{34} + \underline{11} & = \underline{34} - 3(\underline{45} - \underline{34}) \\ \underline{34} = 3 \times \underline{11} + \underline{1} & = 4 \times \underline{34} - 3 \times \underline{45} \\ \underline{11} = 11 \times \underline{1} + 0 & = 4(\underline{79} - \underline{45}) - 3 \times \underline{45} \\ & = 4 \times \underline{79} - 7 \times \underline{45} \end{array}$$

Thus, $c = 4$ is an inverse of 79 modulo 45.

3. From the theorem, we conclude that the solution to our original linear congruence $79x \equiv 12 \pmod{45}$ is

$$x \equiv 4 \times 12 = 48 \equiv 3 \pmod{45}.$$

i.e. $x = \dots, -42, 3, 48, \dots$

Exercise. Solve $23x \equiv 11 \pmod{30}$.

cont'd

Question What if $\gcd(a, m) \neq 1$?

We use the following trick.

● **Theorem.** If $c \neq 0$, then the congruences

$$ax \equiv b \pmod{m} \quad \text{and} \quad cax \equiv cb \pmod{cm}$$

have the same solutions.

★ We can cancel a factor from both sides of a congruence, provided that we cancel it from the modulus as well.

Proof. (Brief sketch) x is a solution to $ax \equiv b \pmod{m}$ iff there's an integer y with $ax - b = my$ iff there's an integer y with $cax - cb = cmy$ iff x is a solution to the congruence equation $cax \equiv cb \pmod{cm}$.

Example. Now we solve the linear congruence

$$52x \equiv 8 \pmod{60}.$$

1. We “divide” by $\gcd(52, 60) = 4$ and use the theorem above to see the congruence equation above has the same solutions as

$$13x \equiv 2 \pmod{15}.$$

2. Now $\gcd(13, 15) = 1$ so we solve the new congruence equation by finding an inverse c of 13 modulo 15 using the Extended Euclidean Algorithm.

$$\underline{15} = 1 \times \underline{13} + \underline{2}$$

$$\underline{13} = 6 \times \underline{2} + \underline{1}$$

$$\underline{2} = 2 \times \underline{1} + 0$$

$$\underline{1} = \underline{13} - 6 \times \underline{2}$$

$$= \underline{13} - 6(\underline{15} - \underline{13})$$

$$= 7 \times \underline{13} - 6 \times \underline{15}$$

We see that $c = 7$ is an inverse of 13 modulo 15.

3. Hence the solutions to $13x \equiv 2 \pmod{15}$ are $x \equiv 7 \times 2 = 14 \pmod{15}$, which is also the solution to the original congruence equation.

4. Equivalently, we can write the solution in terms of the original modulus

$$x \equiv 14, 29, 44, 59 \pmod{60}.$$

5. Note that there are now $4 = \gcd(52, 60)$ solutions modulo 60.

Exercise. Solve the congruence $9x \equiv -3 \pmod{24}$. Give your answer as a congruence to the smallest possible modulus, and as a congruence modulo 24.

cont'd

To summarise

● **Theorem.** Consider the congruence $ax \equiv b \pmod{m}$.

- (i) If $\gcd(a, m) = 1$, then the congruence has a unique solution modulo m .
- (ii) If $\gcd(a, m)$ is not a factor of b , then the congruence has no solution.
- (iii) If $d = \gcd(a, m)$ is a factor of b , then the congruence has
 - one unique solution modulo m/d , and
 - d different solutions modulo m .

Exercise. Without actually solving anything, determine how many solutions the following congruences have. Give your answers in terms of the original modulus, and in terms of a smaller modulus if appropriate.

(a) $15x \equiv 18 \pmod{21}$

(b) $16x \equiv 19 \pmod{22}$

(c) $17x \equiv 20 \pmod{23}$

Sometimes we can solve congruences without using the Euclidean Algorithm but rather using the following fact we have observed before.

● **Theorem.** If $\gcd(c, m) = 1$, then

$$p \equiv q \pmod{m} \quad \text{if and only if} \quad cp \equiv cq \pmod{m}$$

Example.

$$\begin{aligned} 52x &\equiv 4 \pmod{60} \\ \iff 13x &\equiv 1 \pmod{15} \\ \iff -2x &\equiv -14 \pmod{15} \\ \iff x &\equiv 7 \pmod{15} \end{aligned}$$

Exercise. Prove the divisibility by 7 test, namely, $10a + b \equiv 0 \pmod{7}$ if and only if $a - 2b \equiv 0 \pmod{7}$.

Example. Public Key Cryptography – the RSA System was invented by 3 MIT undergraduates (Rivest, Shamir and Adleman) in 1976:

- Find *two large primes* p and q (e.g., 200 digits each).
- Form the *modulus* $m = pq$.
- Find an *encryption exponent* α relatively prime to $(p - 1)(q - 1)$.
- Find the *decryption exponent* β satisfying $\alpha\beta \equiv 1 \pmod{(p - 1)(q - 1)}$.
- Publish the numbers α and m . Forget p and q and keep β secret.

To encrypt...

1. Convert plain text into a string of digits to form a large integer x .
2. Compute $y = (x^\alpha \bmod m)$.
3. Send y .

To decrypt...

1. Receive y .
2. Compute $x = (y^\beta \bmod m)$. Note that you only need to know β .
Uses fact that $x^{(p-1)(q-1)} \equiv 1 \pmod{m}$ (see Epp page 629.).
3. Convert x back to plain text.

Why is this secure?

To decrypt the message we must know β , which can be obtained if p and q are known. Recall that primality testing is much faster than prime factorization. Although it is easy to find two large primes p and q to form the product $m = pq$, it is close to impossible to factorize a large m to find the values of p and q .

NOTE THAT RSA IS NOT EXAMINABLE

RELATIONS

- A **relation** R from a set A to a set B is a **subset of $A \times B$** .
 - If $(a, b) \in R$ we say that **a is related to b (by R)**, and we write **$a R b$** .
 - If $(a, b) \notin R$ we write **$a \not R b$** .
- Representing a relation $R \subseteq A \times B$ on finite sets A and B :
 - **Arrow diagram**: List the elements of A and the elements of B , and then **draw an arrow from a to b for each pair $(a, b) \in R$** .
 - **Matrix M_R** : Arrange the elements of A and B in some order a_1, a_2, \dots and b_1, b_2, \dots , and then form a rectangular array of numbers where

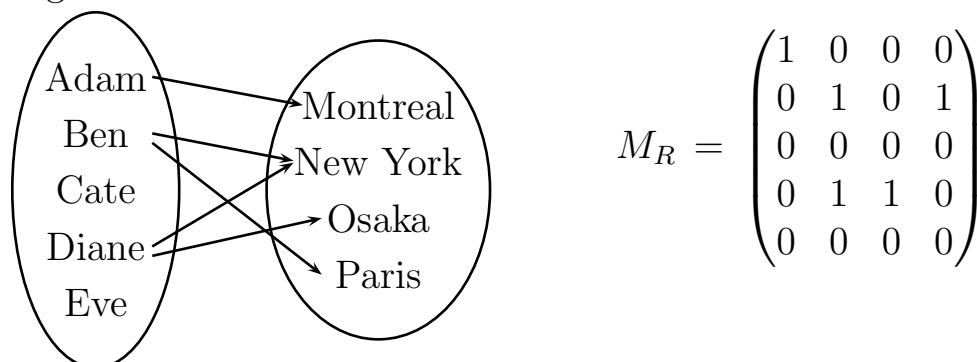
 the entry in the i th row and j th column $= m_{i,j} = \begin{cases} 1 & \text{if } a_i R b_j; \\ 0 & \text{if } a_i \not R b_j. \end{cases}$
 - The matrix M_R has $|A|$ rows and $|B|$ columns.
 - The matrix changes if the elements are arranged in a different order.

Example. Five flatmates Adam, Ben, Cate, Diane, and Eve chatted about who had visited the four cities Montreal, New York, Osaka, and Paris.

Their travel experiences lead to a relation “has visited” defined as follows:

$$\begin{aligned}
 A &= \{\text{Adam, Ben, Cate, Diane, Eve}\} \\
 B &= \{\text{Montreal, New York, Osaka, Paris}\} \\
 R &= \{(\text{Adam, Montreal}), (\text{Ben, New York}), (\text{Ben, Paris}), \\
 &\quad (\text{Diane, New York}), (\text{Diane, Osaka})\}
 \end{aligned}$$

The arrow diagram and matrix for this relation are



The matrix M_R is of size 5×4 (reads “5 by 4”).

It is based on the alphabetical order of the names and cities.

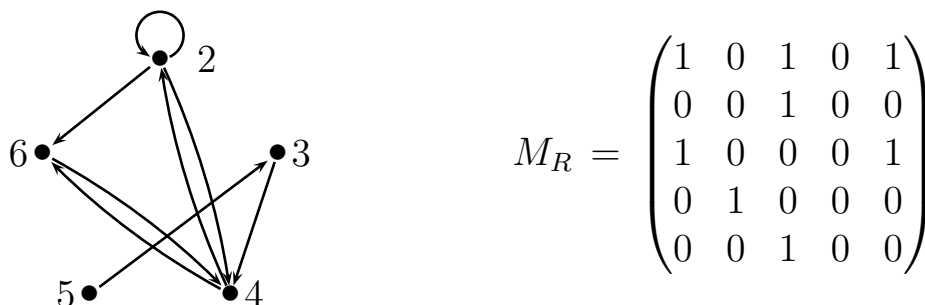
- A **function** is just a relation $R \subseteq A \times B$ with the special property that for every $a \in A$ there is exactly one $b \in B$ such that $a R b$.
- A relation over two sets as defined above is formally a **binary relation**. We can also define a **ternary relation** as a subset of the Cartesian product $A \times B \times C$ of three sets A, B, C , or in general, an **n -ary relation** as a subset of $A_1 \times A_2 \times \cdots \times A_n$ for sets A_1, A_2, \dots, A_n .
- Here we shall consider mainly **binary relations ON a set**, that is, a relation from a set to itself.
 - The arrow diagram in this case is essentially a **directed graph** (see Topic 5). We draw a dot for each element in the set and use an arrow or a loop to represent each ordered pair.
 - The corresponding matrix M_R is a **square** matrix; that is, there are as many rows as there are columns.

Example. We define a relation R on the set $A = \{2, 3, 4, 5, 6\}$ by

$$\begin{aligned} R &= \{(a, b) \in A \times A \mid a \text{ is a factor of } b + 2\} \\ &= \{(2, 2), (2, 4), (2, 6), (3, 4), (4, 2), (4, 6), (5, 3), (6, 4)\}. \end{aligned}$$

Then we can write, for example, $2 R 4$ and $3 R 4$, but $5 \not R 4$.

The arrow diagram and matrix are



Exercise. Let $R = \{(a, a), (a, b), (b, a), (b, b), (d, b)\}$ be a relation on the set $A = \{a, b, c, d\}$. Draw the arrow diagram of R and write down the matrix of R .

- We say that a relation R on a set A is **reflexive** when for every $a \in A$,

$$a R a,$$

i.e., every element is related to itself.

- We say that a relation R on a set A is **symmetric** when for every $a, b \in A$,

$$a R b \quad \text{implies} \quad b R a,$$

i.e., if a is related to b , then b is related to a .

- We say that a relation R on a set A is **antisymmetric** when for every $a, b \in A$,

$$a R b \quad \text{and} \quad b R a \quad \text{implies} \quad a = b,$$





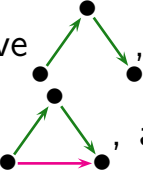



i.e., if a and b are related to each other, then they must be identical.

- We say that a relation R on a set A is **transitive** when for every $a, b, c \in A$,

$$a R b \quad \text{and} \quad b R c \quad \text{implies} \quad a R c,$$

i.e., if a is related to b and b is related to c , then a is related to c .

- In terms of arrow diagrams and matrices...

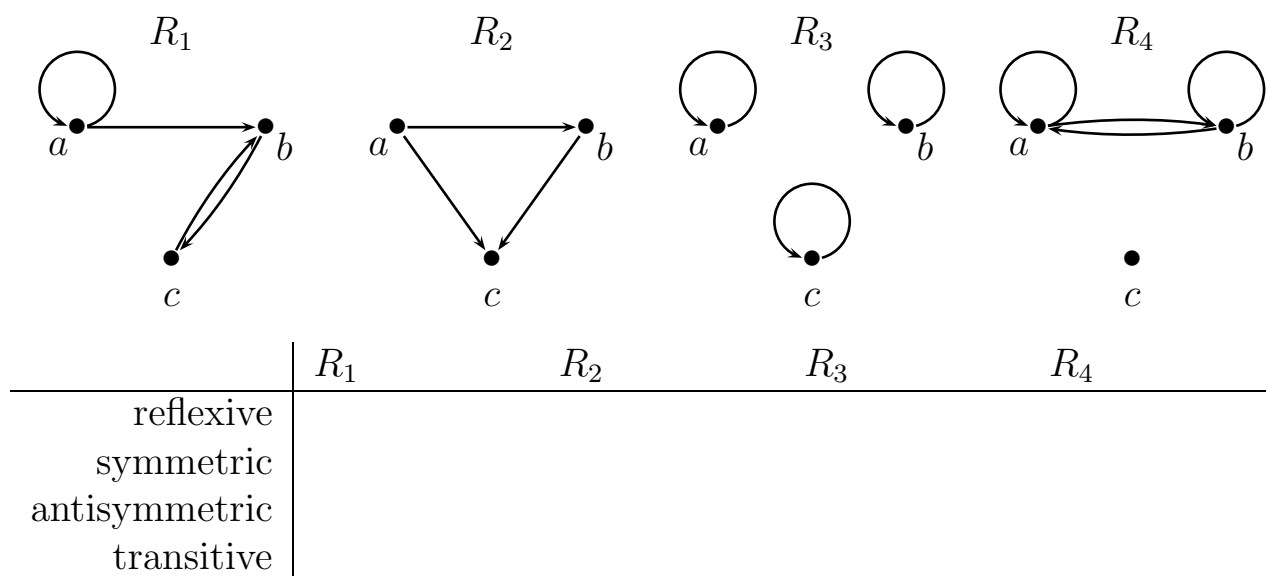
	arrow diagram	matrix
reflexive	we must have  at every dot	diagonal entries are all 1
symmetric	if we have  , then we must have 	for $i \neq j$, $m_{i,j} = m_{j,i}$
antisymmetric	we cannot have 	for $i \neq j$, $m_{i,j}$ and $m_{j,i}$ cannot both be 1
transitive	<p>(i) if we have , then we must have , and</p> <p>(ii) if we have , then we must have </p>	for every nonzero entry in the matrix product M^2 the corresponding entry in M must be 1

- Note that “antisymmetric” is not the opposite of “symmetric”. A relation can be both symmetric and antisymmetric.

Exercise. Define the relations R_1, R_2, R_3, R_4 on the set $A = \{a, b, c\}$ by

$$\begin{aligned} R_1 &= \{(a, a), (a, b), (b, c), (c, b)\}, & R_2 &= \{(a, b), (a, c), (b, c)\}, \\ R_3 &= \{(a, a), (b, b), (c, c)\}, & R_4 &= \{(a, a), (a, b), (b, a), (b, b)\}. \end{aligned}$$

For each relation, determine whether it is reflexive, symmetric, antisymmetric, and/or transitive.



Exercise. For each relation R defined on the set of all human beings, determine whether or not it is reflexive, symmetric, antisymmetric, or transitive.

$(a, b) \in R$ if and only if	reflexive	symmetric	antisymmetric	transitive
a is the father of b				
a is a sibling of b				
a is taller than b				

Exercise. For each relation R defined on the set of all integers, determine whether or not it is reflexive, symmetric, antisymmetric, or transitive.

$(x, y) \in R$ if and only if	reflexive	symmetric	antisymmetric	transitive
(a) $x = y$				
(b) $x > y$				
(c) $x \leq y$				
(d) $x \neq y$				
(e) Fix integer $m \geq 2$. $x \equiv y \pmod{m}$				
(f) x is a multiple of y				
Give reasons for (e).				

Reasons

- A reflexive, symmetric, and transitive relation is called an *equivalence relation*.
- We often write \sim to denote an equivalence relation:
 $a \sim b$ reads “ a is *equivalent* to b ” (with respect to \sim).
- Intuitively, an equivalence relation tells us when two things are “the same” in an appropriate way.

Example. Two angles (in radians) which differ by an integer multiple of 2π are essentially “the same”. We can express this idea using the relation \sim on \mathbb{R} defined by

$$x \sim y \quad \text{if and only if} \quad \frac{x - y}{2\pi} \in \mathbb{Z}.$$

1. For all $x \in \mathbb{R}$, clearly $\frac{x-x}{2\pi} = 0 \in \mathbb{Z}$ so $x \sim x$ and \sim is reflexive.
2. Suppose that $x \sim y$ so that $\frac{x-y}{2\pi} \in \mathbb{Z}$. Then its negative $\frac{y-x}{2\pi} \in \mathbb{Z}$. Thus $y \sim x$ and \sim is symmetric.
3. Suppose that $x \sim y$ and $y \sim z$ for some $x, y, z \in \mathbb{R}$. Then $\frac{x-y}{2\pi}, \frac{y-z}{2\pi} \in \mathbb{Z}$. Hence, their sum $\frac{x-z}{2\pi} \in \mathbb{Z}$ so $x \sim z$. Thus, \sim is transitive.

Since \sim is reflexive, symmetric, and transitive, it is an equivalence relation. Two real numbers are equivalent with respect to \sim if they represent the same angle.

- Let \sim be an equivalence relation on a set A . For any element $a \in A$, the *equivalence class* of a with respect to \sim , denoted by $[a]$, is the set

$$[a] = \{x \in A \mid x \sim a\}.$$

- Intuitively, an equivalence class collects all the objects that are “the same” so that we can regard them as a single object.
- We let A/\sim denote the *set of equivalence classes*. Thus $A/\sim \subseteq P(A)$.

Example. For the equivalence relation \sim in the previous example, a typical element of \mathbb{R}/\sim is an equivalence class like

$$\left[\frac{\pi}{2}\right] = \left\{\dots, -\frac{3\pi}{2}, \frac{\pi}{2}, \frac{5\pi}{2}, \frac{9\pi}{2}, \dots\right\} \quad \text{or} \quad \left[\frac{\pi}{4}\right] = \left\{\dots, -\frac{7\pi}{4}, \frac{\pi}{4}, \frac{9\pi}{4}, \frac{17\pi}{4}, \dots\right\}.$$

Elements of \mathbb{R}/\sim represent angles.

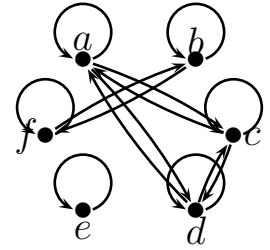
Functions with period 2π like sine and cosine are functions of angles and thus functions on \mathbb{R}/\sim . For example, we can define $\cos : \mathbb{R}/\sim \rightarrow \mathbb{R}$ by

$$\cos([a]) = \cos a' \quad \text{for any } a' \in [a].$$

Note that the choice of a' doesn't affect the definition because \cos has period 2π .

Example. Let $A = \{a, b, c, d, e, f\}$ and

$$R = \{(a, a), (a, c), (a, d), (b, b), (b, f), (c, a), (c, c), (c, d), (d, a), (d, c), (d, d), (e, e), (f, b), (f, f)\}.$$



Since R is reflexive, symmetric, and transitive, it is an equivalence relation. The equivalence classes are

$$\begin{aligned} [a] &= \{a, c, d\}, & [b] &= \{b, f\}, & [c] &= \{a, c, d\}; \\ [d] &= & [e] &= & [f] &= \end{aligned}$$

In particular, we have $[a] = [c] = [d]$ and $[b] = [f]$.

● **Theorem.** Let \sim be an equivalence relation on a set A . Then

(i) For all $a \in A$, $a \in [a]$. Hence,

- ★ every element of A belongs to at least one equivalence class.
- ★ every equivalence class contains at least one element.

(ii) For all $a, b \in A$, $a \sim b$ if and only if $[a] = [b]$.

(iii) For all $a, b \in A$, $a \not\sim b$ if and only if $[a] \cap [b] = \emptyset$.

- ★ Hence any two equivalence classes are either equal or disjoint.

Proof.

(i) Since \sim is reflexive, for every element a we have $a \sim a$ and so $a \in [a]$.

(ii) Let $a \sim b$. Suppose $x \in [a]$, which means $x \sim a$. Since \sim is transitive, we have $x \sim b$, which leads to $x \in [b]$. Thus, $[a] \subseteq [b]$. Similarly, we can show that $[b] \subseteq [a]$. Hence, $a \sim b$ implies that $[a] = [b]$.

Now let $[a] = [b]$. By i) we have $a \in [a]$ so $a \in [b]$. Thus $a \sim b$ and $[a] = [b]$ implies $a \sim b$.

Hence, $a \sim b$ if and only if $[a] = [b]$.

(iii) Let $a \not\sim b$. Suppose $[a] \cap [b] \neq \emptyset$ so there's some $x \in [a] \cap [b]$. Then $x \in [a]$ and $x \in [b]$. Then $x \sim a$ and $x \sim b$. Since \sim is symmetric, we have $a \sim x$ and $x \sim b$. Since \sim is transitive, we have $a \sim b$. This contradicts the fact that $a \not\sim b$. Hence, if $a \not\sim b$, then $[a] \cap [b] = \emptyset$.

Now let $[a] \cap [b] = \emptyset$. Suppose $a \sim b$. Then by (ii) and (i) we have $[a] = [b] \neq \emptyset$. This contradicts $[a] \cap [b] = \emptyset$. Thus, if $[a] \cap [b] = \emptyset$, then $a \not\sim b$.

Hence, $a \not\sim b$ if and only if $[a] \cap [b] = \emptyset$.

● A **partition** of a set A is a collection of disjoint nonempty subsets of A whose union equals A . When this holds, we say that these sets **partition** A .

Example. Let $A = \{a, b, c, d, e, f\}$. The subsets

$$\{a, c, d\}, \{b, f\}, \{e\}$$

partition A . Note these were the equivalence classes in the previous example.

● **Theorem.** Let A be a set.

- (i) The equivalence classes of an equivalence relation on A partition A .
- (ii) Any partition of A can be used to form an equivalence relation on A .

Proof.

(i) Since every element of A belongs to some equivalence class, we have that the union of the equivalence classes equals A . Since the equivalence classes are either equal or disjoint, we conclude that the equivalence classes partition A .

(ii) Suppose that we have a partition of A , that is, we have a collection of disjoint nonempty subsets of A whose union equals A .

We define a relation \sim on A by

$$a \sim b \quad \text{if and only if} \quad a \text{ and } b \text{ belong to the same subset.}$$

1. For any $a \in A$, since a belongs to one of these subsets we have $a \sim a$. Thus, \sim is reflexive.
2. For any $a, b \in A$, if a and b belong to the same subset, then b and a belong to the same subset. Thus, \sim is symmetric.

3. For any $a, b, c \in A$, if a and b belong to the same subset and b and c belong to the same subset, then all three elements belong to the same subset, and in particular, a and c belong to the same subset. Thus, \sim is transitive.

Hence, \sim is an equivalence relation on A .

Example. Let m be a positive integer. We saw in a previous exercise that the relation “*congruence modulo m* ” on the set of integers, that is,

$$a \sim b \quad \text{if and only if} \quad a \equiv b \pmod{m},$$

is reflexive, symmetric and transitive. It is thus an equivalence relation. For $m = 2$, we get a partition of \mathbb{Z} into

$$[0] = [2] = \dots = \quad \text{the set of even numbers and}$$

$$[1] = [3] = \dots = \quad \text{the set of odd numbers}$$

Exercise. List the equivalence classes for the case $m = 3$.

Exercise. List all equivalence relations on the set $A = \{1, 2, 3\}$.

- A reflexive, antisymmetric, and transitive relation is called a *partial order*.
- We often write \preceq to denote a partial order: $a \preceq b$ reads “ a *precedes* b ”.
- Intuitively, a partial ordering tells us which of two things “comes first” with respect to the particular way of ordering things.

Example. Consider the relation \leq on the set of real numbers \mathbb{R} .

1. For any $a \in \mathbb{R}$, we have $a \leq a$. Thus, \leq is reflexive.
2. For any $a, b \in \mathbb{R}$, if $a \leq b$ and $b \leq a$, then $a = b$. Thus, \leq is antisymmetric.
3. For any $a, b, c \in \mathbb{R}$, if $a \leq b$ and $b \leq c$, then $a \leq c$. Thus, \leq is transitive.

Since \leq is reflexive, antisymmetric, and transitive, it is a partial order on \mathbb{R} . $a \leq b$ means that a comes before b if we list the numbers in increasing order.

Example. The relation \geq is a partial ordering on the set of real numbers \mathbb{R} . $a \geq b$ means that a comes before b if we list the numbers in decreasing order.

Exercise. Prove that divisibility $|$ defines a partial order on the set of positive integers \mathbb{Z}^+ .

Exercise. For any set S , prove that the relation \subseteq is a partial order on $P(S)$.

- A set A together with a partial order \preceq is called a *partially ordered set* or a *poset*. We denote this by (A, \preceq) .
- We say that two elements $a, b \in A$ are *comparable* with respect to a partial order \preceq if and only if *at least one of $a \preceq b$ or $b \preceq a$ holds*.
- A partial order in which *every pair of two elements are comparable* is called a *total order* or a *linear order*.

Example. (\mathbb{R}, \leq) is a poset. Moreover, \leq is a total order on \mathbb{R} . Similarly, (\mathbb{R}, \geq) is a totally ordered set.

Example. $(\mathbb{Z}^+, |)$ is a poset but not a total order. For instance, $2 \nmid 7$ and $7 \nmid 2$, so 2 and 7 are not comparable in this poset.

Exercise. We have shown earlier that $(P(S), \subseteq)$ is a poset for any set S . Is the relation \subseteq a total order on $P(S)$?

Example. On the set $\mathbb{R} \times \mathbb{R}$, we define

$$(z, z') \preceq (w, w') \quad \text{if and only if} \quad z \leq w \text{ and } z' \leq w'.$$

Prove that \preceq is a partial order on $\mathbb{R} \times \mathbb{R}$ but not a total order.

1. For any $(z, z') \in \mathbb{R} \times \mathbb{R}$, we have $z \leq z$ and $z' \leq z'$, and so $(z, z') \preceq (z, z')$. Thus, \preceq is reflexive.
2. Let $(z, z'), (w, w') \in \mathbb{R} \times \mathbb{R}$ and suppose that $(z, z') \preceq (w, w')$ and $(w, w') \preceq (z, z')$. Then $z \leq w$ and $z' \leq w'$, and $w \leq z$ and $w' \leq z'$. Thus, $z = w$ and $z' = w'$, which leads to $(z, z') = (w, w')$. Hence $(z, z') \preceq (w, w')$ and $(w, w') \preceq (z, z')$ imply $(z, z') = (w, w')$, so we conclude that \preceq is antisymmetric.
3. Let $(z, z'), (w, w'), (u, u') \in \mathbb{R} \times \mathbb{R}$ and suppose that $(z, z') \preceq (w, w')$ and $(w, w') \preceq (u, u')$. Then $z \leq w$ and $z' \leq w'$, and $w \leq u$ and $w' \leq u'$. Thus, $z \leq u$ and $z' \leq u'$ so $(z, z') \preceq (u, u')$. We conclude that \preceq is transitive.

Since \preceq is reflexive, antisymmetric, and transitive, it is a partial order on $\mathbb{R} \times \mathbb{R}$.

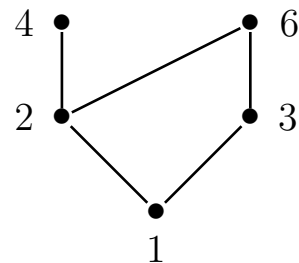
\preceq is not a total order on $\mathbb{R} \times \mathbb{R}$. For example, $(2, 3)$ and $(3, 2)$ are not comparable.

- We can represent a partial order \preceq on a finite set by a *Hasse diagram*:
 - If $a \preceq b$ and $a \neq b$ (in which case, we often write $a \prec b$), then we draw a line between a and b , with a positioned lower than b in the diagram.
 - We do not draw any lines that can be deduced by the transitive property: $a \preceq b$ and $b \preceq c$ imply $a \preceq c$.
 - We do not draw any loops to indicate the reflexive property $a \preceq a$.

Example. $(\{1, 2, 3, 4, 6\}, |)$ is a poset. More precisely, the relation is

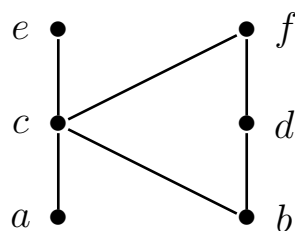
$$R = \{(1, 1), (1, 2), (1, 3), (1, 4), (1, 6), (2, 2), (2, 4), (2, 6), (3, 3), (3, 6), (4, 4), (6, 6)\}.$$

The corresponding Hasse diagram is



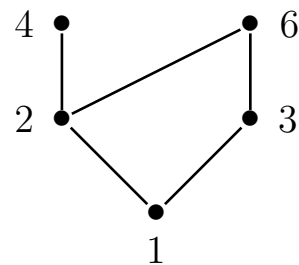
Exercise. Draw the Hasse diagram for the poset $(P(S), \subseteq)$ where $S = \{a, b, c\}$.

Exercise. Determine the poset represented by the following Hasse diagram.



- Let (A, \preceq) be a poset. An element $x \in A$ is called
 - a *maximal element* iff there is no element $a \in A$ with $x \prec a$;
 - a *minimal element* iff there is no element $a \in A$ with $a \prec x$;
 - the *greatest element* iff $a \preceq x$ for all $a \in A$;
 - the *least element* iff $x \preceq a$ for all $a \in A$.
 - ★ The greatest element in a poset is unique if it exists.
 - ★ The least element in a poset is unique if it exists.
- Let $S \subseteq A$.
 - an *upper bound for S* is an element $b \in A$ such that $s \preceq b$ for every $s \in S$.
 - a *lower bound for S* is an element $b \in A$ such that $b \preceq s$ for every $s \in S$.
 - the *least upper bound for S* (if it exists) is the least element for the set of upper bounds.
 - the *greatest lower bound for S* (if it exists) is the greatest element for the set of lower bounds.

Example. Consider the poset $(\{1, 2, 3, 4, 6\}, |)$:



The maximal elements are 4 and 6.

The minimal element is 1.

There is no greatest element.

The least element is 1.

The set of upper bounds for $\{1, 2\}$ is $\{2, 4, 6\}$.

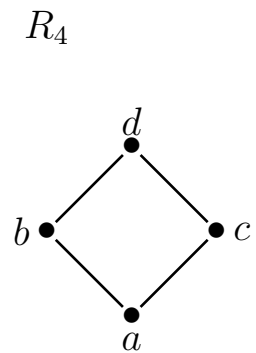
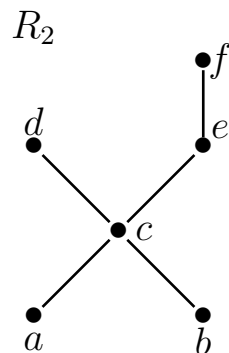
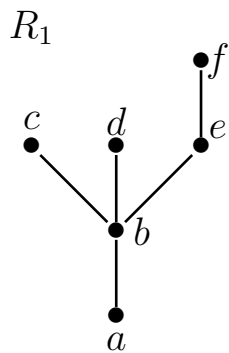
The least upper bound for $\{1, 2\}$ exists and is 2.

The set $\{3, 4\}$ has no upper bounds.

The set of lower bounds for $\{4, 6\}$ is $\{1, 2\}$.

The greatest lower bound for $\{4, 6\}$ exists and is 2.

Exercise. For the posets represented by the following Hasse diagrams, list the maximal, minimal, greatest and least elements if they exist.



	R_1	R_2	R_3	R_4
maximal elements				
minimal elements				
greatest element				
least element				
l.u.b. $\{a, b\}$				

Exercise. Draw the Hasse diagram for the divisibility relation on the set

$$S = \{\text{positive factors of } 72\}.$$