



CONTENTS

1	Triangles, Angles, and Parallels	5
1.1	Angles	5
1.1.1	Radians	7
1.2	Introduction to Triangles	8
1.2.1	Equilateral, Isosceles, and Scalene Triangles	8
1.2.2	Interior Angles of a Triangle	10
1.2.3	Is it an Equilateral, Isosceles, or Scalene Triangle with <i>Python</i> ?	12
1.3	Pythagorean Theorem	13
1.3.1	Distance between Points	15
1.3.2	Distance in 3 Dimensions	17
1.4	Parallel and Perpendicular	17
2	Congruence	19
2.1	Rigid Transformations	19
2.2	Triangle Congruency	20
3	Circles	25
3.1	Arc Length	27
3.2	Sector Area	30
3.3	Secants and Tangents	32
4	Functions and Their Graphs	35
4.1	Graphs of Functions	36
4.2	Can this be expressed as a function?	38

4.3	Graphing Calculators	38
4.4	Even and Odd Functions	41
4.4.1	Even Functions	41
4.4.2	Odd Functions	41
4.4.3	Neither Even Nor Odd	42
4.5	Piecewise Functions	44
4.5.1	Floor and Ceiling Functions	46
4.5.2	Invalid Piecewise Functions	48
4.6	Summary	51
5	Inverses and Transformations	53
5.1	Inverses	53
5.2	Transforming Functions	57
5.2.1	Translation up and down	59
5.2.2	Translation left and right	59
5.2.3	Scaling up and down in the y direction	60
5.2.4	Scaling up and down in the x direction	60
5.2.5	Order is important!	62
5.2.6	Effects on even and odd Functions	64
6	Solving Quadratics	65
6.1	Completing the Square	65
6.2	The Traditional Quadratic Formula	68
6.3	Factoring Quadratics	69
7	Number Theory and Cryptography	73
7.1	Divisibility	73
7.1.1	The Division Algorithm	73
7.2	Prime Numbers	74
7.2.1	There Are Infinitely Many Primes	75
7.2.2	Testing Whether a Number Is Prime	75
7.2.3	The Sieve of Eratosthenes	75
7.3	The Greatest Common Divisor	76
7.3.1	The Euclidean Algorithm	76
7.3.2	The Extended Euclidean Algorithm	77
7.4	Modular Arithmetic	78
7.4.1	Modular Inverses	79
7.4.2	Fast Powers	80
7.5	Fermat's Little Theorem	80

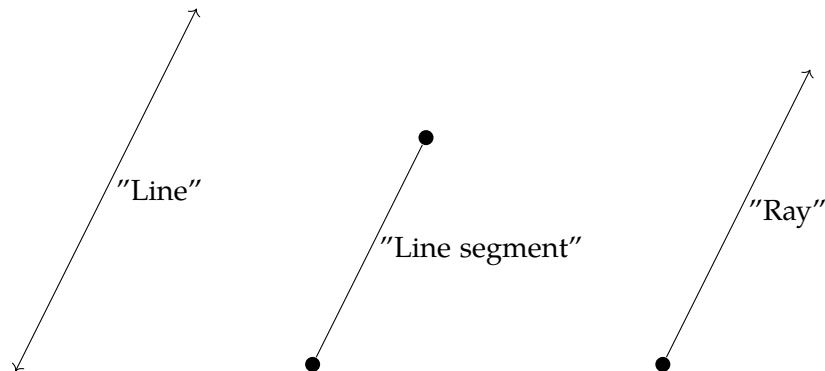
		3
	7.5.1 A Fast Primality Test	81
7.6	RSA	82
	7.6.1 Making the Keys	82
	7.6.2 Why Decryption Works	83
	7.6.3 Why It Is Secure	83
A	Answers to Exercises	87
Index		103

CHAPTER 1

Triangles, Angles, and Parallels

1.1 Angles

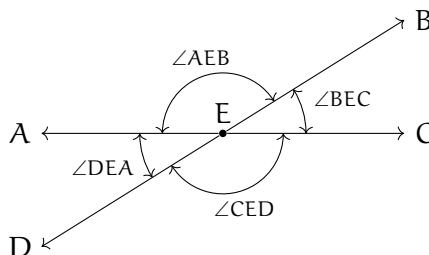
In the following recommended videos, the narrator talks about lines, line segments, and rays. When mathematicians talk about *lines*, they mean a straight line that goes forever in two directions. If you pick any two points on that line, the space between them is a *line segment*. If you take any line, pick a point on it, and discard all the points on one side of the point, that is a *ray*. All three have no width.



Watch the following videos from Khan Academy:

- Introduction to angles: <https://youtu.be/H-de6Tkxej8>
- Measuring angles in degrees: <https://youtu.be/92aLiyeQj0w>

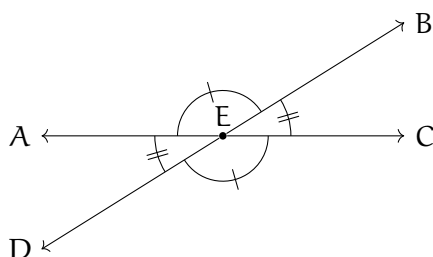
When two lines cross, they form four angles:



What do we know about those angles? (Note that $m\angle$ means "the measure of angle")

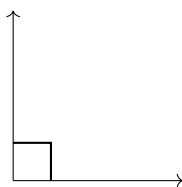
- The sum of any two adjacent angles adds to be 180° . So, for example, $m\angle AEB + m\angle BEC = 180^\circ$. We use the phrase “adds to be 180° ” so often that we have a special word for it: *supplementary*.
- The sum of all four angles is 360° .
- Angles opposite each other are equal. So, for example, $m\angle AEB = m\angle CED$.
- Angles that sit side by side along a straight line add up to 180° . For example, the angles on one side of $\overline{AC}$ add up to 180° .

In a diagram, to indicate that two angles are equal we often put hash marks in the angle:



Here, the two angles with a single hash mark are equal, and the two angles with double hash marks are equal.

When two lines are perpendicular, the angle between them is 90° , and we say they meet at a *right angle*. When drawing diagrams, we indicate right angles with an elbow:

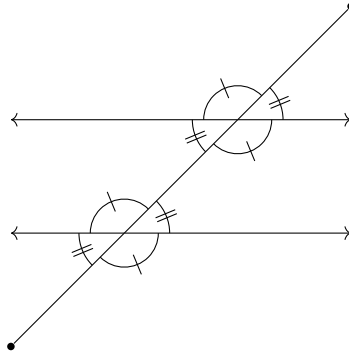


When an angle is less than 90° , it is said to be *acute*. When an angle is more than 90° , it is said to be *obtuse*.

Just as two angles which add up to 180° are referred to as supplementary angles, two (or more) angles which add up to 90° are *complementary* angles. For example, two 45° angles are complementary, as well as 30° and 60° . If an angle is 65° , we say that its *complement* is $90^\circ - 65^\circ = 25^\circ$.



If two lines are parallel (never intersecting lines with points all the same distance apart), line segments that intersect both lines (transversals) form the same angles with each line:



1.1.1 Radians

As you have seen above, angles can be measured in degrees. Just like you can measure length in more than one unit (inches, meters, etc.), there is more than one unit to measure angles in. Angles can also be measured in *radians*. Radians are unitless (that is, you do not have to put a letter after the number) and there are π radians across a straight line. On diagrams and equations, unknown angles in radians are usually represented with the greek letter θ . This means 180° is the same as π radians. Radians come from comparing the length of an arc to the radius of a circle—which we will explore in a future chapter.

Generally, you can use the following formula for your conversions:

$$\text{angle in degrees} = \text{angle in radians} \cdot \frac{180^\circ}{\pi}$$

Example: An angle is measured to be $\frac{\pi}{2}$ radians. What is the angle in degrees?

Solution: Since we know that π radians is the same as 180° , we can set up the unit conversion:

$$\frac{\pi}{2} \cdot \frac{180^\circ}{\pi} = 90^\circ$$

Therefore, a $\frac{\pi}{2}$ angle is 90° .

Exercise 1

Convert the following angles from degrees to radians, or from radians to degrees.

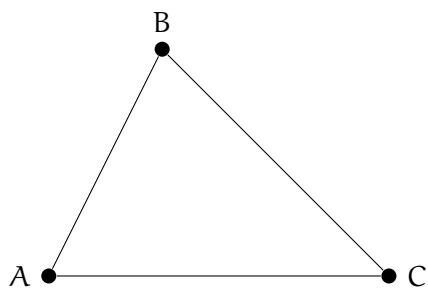
1. 360°
2. $\frac{\pi}{3}$
3. 225°
4. $\frac{3\pi}{4}$
5. 30°
6. 45°

Working Space

Answer on Page 87

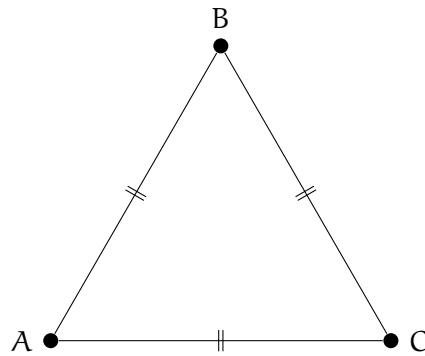
1.2 Introduction to Triangles

Connecting any three points with three line segments will get you a triangle. Here is the triangle ABC, which was created by connecting three points A, B, and C:

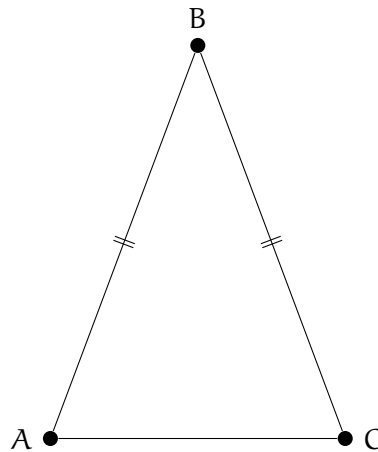


1.2.1 Equilateral, Isosceles, and Scalene Triangles

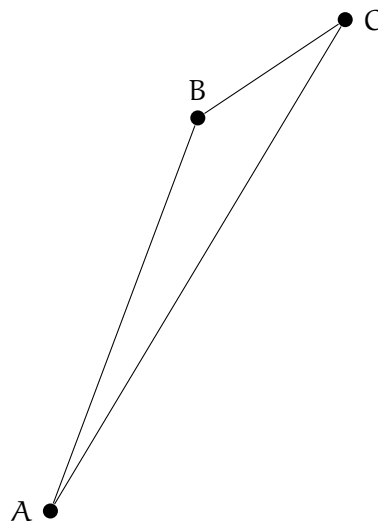
We talk a great deal about the length of the sides of triangles. If all three sides of the triangle are the same length, we say it is an *equilateral triangle*:



If only two sides of the triangle are the same length, we say it is an *isosceles triangle*:

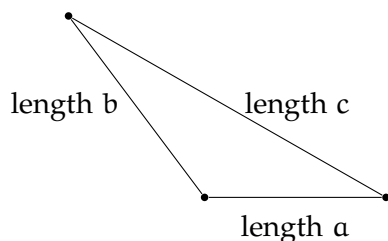


When all three sides of a triangle are different, the triangle is referred to as *scalene*. This consequently means all angle measures are different as well.



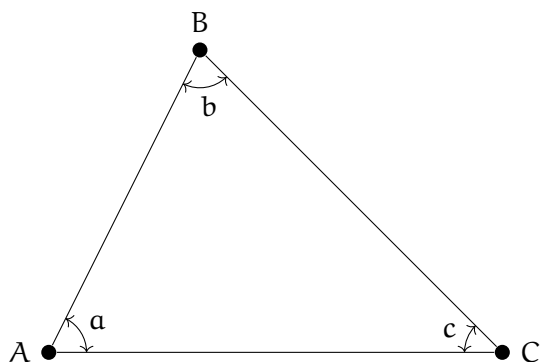
The shortest distance between two points is always the straight line between them. This means you can be certain that the length of one side will *always* be less than the sum of the lengths of the remaining two sides. This is known as the *triangle inequality*.

For example, in this diagram, c must be less than $a + b$.

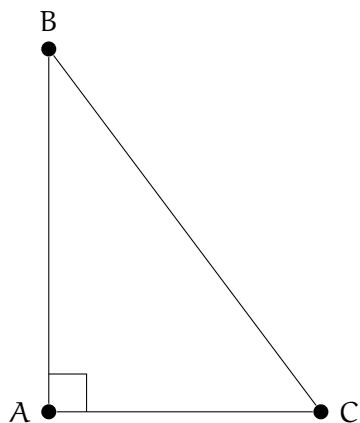


1.2.2 Interior Angles of a Triangle

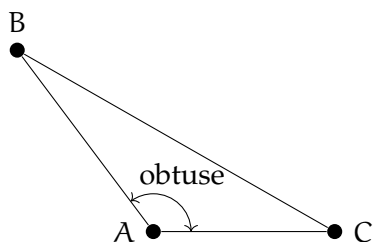
We also talk a lot about the interior angles of a triangle:



A triangle where one of the interior angles is a right angle is said to be a *right triangle*. The side opposite the right angle is the longest side, referred to as the hypotenuse.



If a triangle has an obtuse interior angle, it is said to be an *obtuse triangle*:



If all three interior angles of a triangle are less than 90° , it is said to be an *acute triangle*.

The measures of the interior angles of a triangle always add up to 180° . For example, if we know that a triangle has interior angles of 37° and 56° , we know that the third interior angle is 87° .

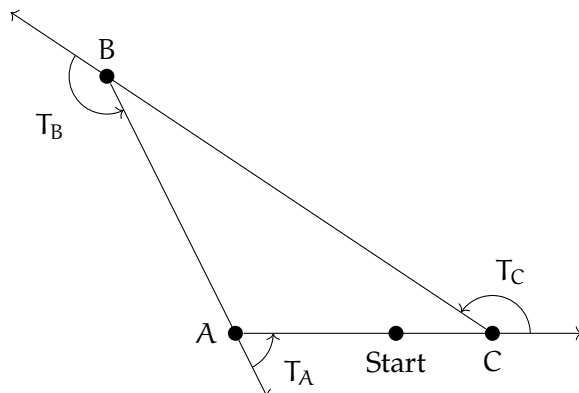
Exercise 2 Missing Angle

One interior angle of a triangle is 92° . The second angle is 42° . What is the measure of the third interior angle?

Working Space

Answer on Page 87

How can you know that the sum of the interior angles is 180° ? Imagine that you started on the edge of a triangle and walked all the way around to where you started, going counter-clockwise. You would turn left three times:



After these three turns, you would be facing the same direction that you started in. Thus, $T_A + T_B + T_C = 360^\circ$. The measures of the interior angles are a , b , and c . Notice that a

and T_A are supplementary. So we know that:

- $T_A = 180 - a$
- $T_B = 180 - b$
- $T_C = 180 - c$

So we can rewrite the equation above as

$$(180 - a) + (180 - b) + (180 - c) = 360^\circ$$

Which simplifies to:

$$540^\circ - (a + b + c) = 360^\circ$$

Rearranging:

$$a + b + c = 180^\circ$$

Exercise 3 Interior Angles of a Quadrilateral

Any four-sided polygon is a *quadrilateral*. Using the same “walk around the edge” logic, what is the sum of the interior angles of any quadrilateral?

Working Space

Answer on Page 87

1.2.3 Is it an Equilateral, Isosceles, or Scalene Triangle with Python?

You have now seen three ways to classify a triangle by its sides, and one rule that decides whether three lengths make a triangle at all. A short Python function can apply both ideas to any triple of numbers you hand it.

```
1 def classify_triangle(a, b, c):
2     short1, short2, longest = sorted([a, b, c])
3     if short1 + short2 <= longest:
4         return "not a triangle"
5     if a == b == c:
6         return "equilateral"
7     if a == b or b == c or a == c:
8         return "isosceles"
```

```
9 |     return "scalene"
```

Sorting the three lengths puts the two shortest sides first, no matter what order they were given in. The triangle inequality check then compares those two shortest sides against the longest one, exactly as stated earlier in this chapter: the length of one side must always be less than the sum of the other two. Once that check passes, the function looks for three equal sides, then two, and falls back to scalene if neither pattern matches.

```
1 | triangles = [(5, 5, 5), (5, 5, 8), (5, 12, 13), (2, 2, 5)]
2 | for sides in triangles:
3 |     print(sides, classify_triangle(*sides))
```

This prints:

```
(5, 5, 5) equilateral
(5, 5, 8) isosceles
(5, 12, 13) scalene
(2, 2, 5) not a triangle
```

Notice the last line. $2 + 2 = 4$, which is not greater than 5, so these three lengths cannot close into a triangle at all, and the function catches that before it ever checks for equal sides.

Exercise 4 Classifying Triangles

Classify each of these triples by hand, then check your answers by running them through `classify_triangle`: (7,7,10), (9,40,41), and (3,4,9).

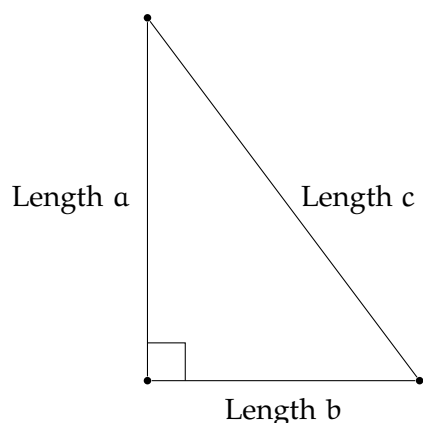
Working Space

Answer on Page 87

1.3 Pythagorean Theorem

Watch Khan Academy's Intro to the Pythagorean Theorem video at <https://youtu.be/AA6RfgP-AHU>.

If you have a right triangle, the edges that touch the right angle are called *the legs*. The third edge, which is always the longest and opposite the right angle, is known as *the hypotenuse*. The Pythagorean Theorem gives us the relationship between the length of the legs and the length of the hypotenuse.



The Pythagorean Theorem tells us that $a^2 + b^2 = c^2$, given that c is the hypotenuse.

For example, if one leg has a length of 3 and the other has a length of 4, then $a^2 + b^2 = 3^2 + 4^2 = 25$. Thus, c^2 must equal 25. This means you know the hypotenuse must be of length 5. This works for any right triangle.

In reality, it rarely works out to be such a tidy number. For example, what is the length of the hypotenuse if the two legs are 3 and 6? $a^2 + b^2 = 3^2 + 6^2 = 45$. The length of the hypotenuse is the square root of that: $\sqrt{45} = \sqrt{9 \times 5} = 3\sqrt{5}$, which is approximately 6.708.

Sets of three whole numbers that fit $a^2 + b^2 = c^2$ are called *Pythagorean triples*. The most famous are (3, 4, 5), (5, 12, 13), and (8, 15, 17). Multiply a triple by any whole number and you get another one: (3, 4, 5) gives (6, 8, 10). Carpenters still use a 3-4-5 triangle to check that a corner is square.

Two right triangles are special because of their angles: the 45° - 45° - 90° triangle and the 30° - 60° - 90° triangle. Their sides are *not* whole numbers; they are in the ratios $1 : 1 : \sqrt{2}$ and $1 : \sqrt{3} : 2$. You will lean on them constantly in trigonometry.

Exercise 5 Find the Missing Length

What is the missing measure? All missing values should be whole numbers, except if it is an irrational number; answer should be a decimal approximation.

Working Space

Leg 1 = 6, Leg 2 = 8, Hypotenuse = a

Leg 1 = 5, Leg 2 = b , Hypotenuse = 13

Leg 1 = c , Leg 2 = 15, Hypotenuse = 17

Leg 1 = 3, Leg 2 = 3, Hypotenuse = d

Answer on Page 87

A square's diagonal is a special case of the Pythagorean Theorem such that $c = \sqrt{a^2 + b^2} = \sqrt{2s^2}$.

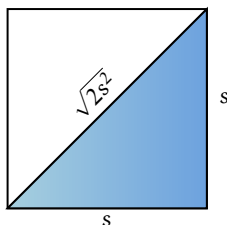
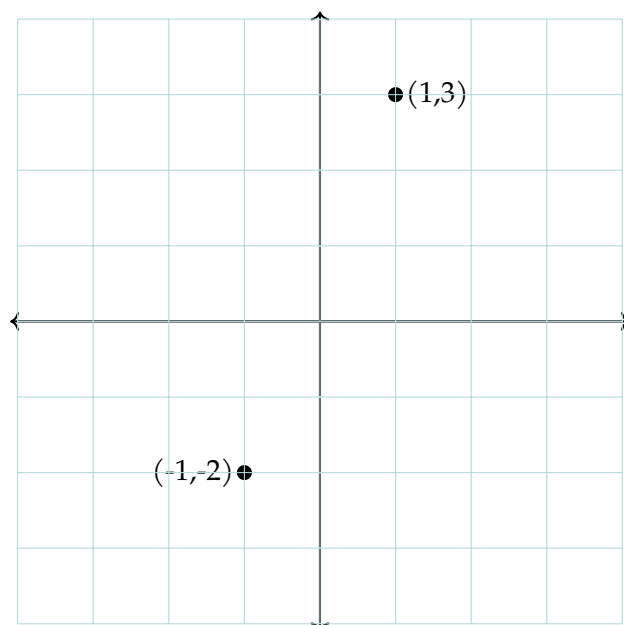


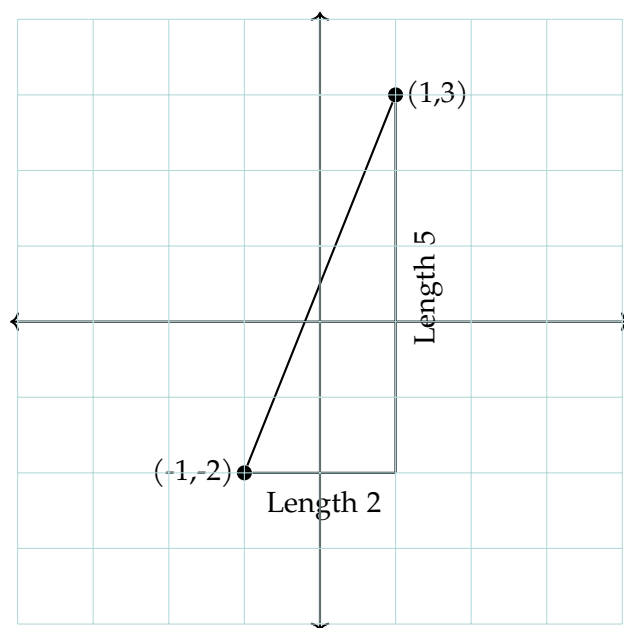
Figure 1.1: A special case of the Pythagorean Theorem where each side is side length s and the hypotenuse is $\sqrt{2s^2}$.

1.3.1 Distance between Points

What is the distance between these two points?



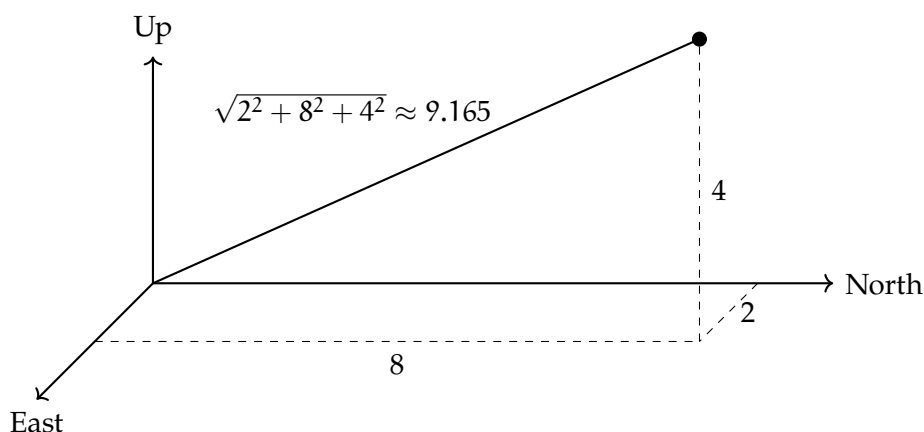
We can draw a right triangle and use the Pythagorean Theorem:



The distance between the two points is $\sqrt{2^2 + 5^2} = \sqrt{29} \approx 5.385165$. In other words, you square the change in x and add it to the square of the change in y . The distance is the square root of that sum.

1.3.2 Distance in 3 Dimensions

What if the point is in three-dimensional space? For example, you move 2 meters East, 8 meters North, and 4 meters up in the air. How far are you from where you started? You just square each, sum them, and take the square root: $\sqrt{2^2 + 8^2 + 4^2} = \sqrt{84} = 2\sqrt{21} \approx 9.165$ meters.



This leads us to a formal definition of the distance formula:

$$d = \sqrt{(x_2 - x_1)^2 + (y_2 - y_1)^2}$$

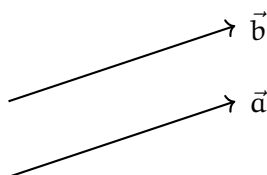
Or in 3D space:

$$d = \sqrt{(x_2 - x_1)^2 + (y_2 - y_1)^2 + (z_2 - z_1)^2}$$

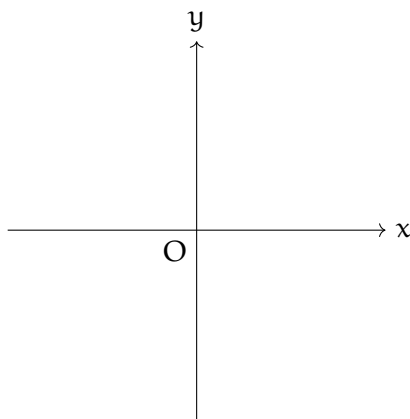
1.4 Parallel and Perpendicular

A *vector* is an arrow: it has a length, called its *magnitude*, and a direction. Velocity, force, and displacement are all vectors.

Two vectors are *parallel* if they point in the same direction or in exactly opposite directions; their lengths do not matter. Two cars driving north are moving in parallel, and so are a car driving north and a car driving south.



Two vectors are *perpendicular* if they meet at a right angle, like the x - and y -axes, or the edges of a sheet of paper.

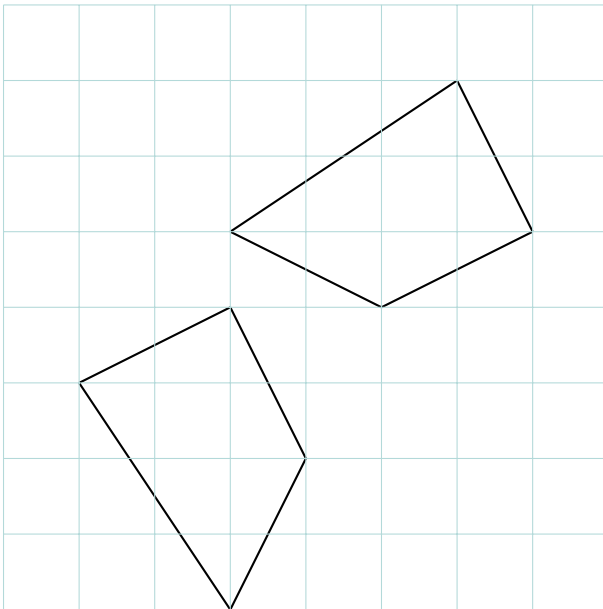


Perpendicular vectors have a handy property: their *dot product* is zero. You will learn the dot product in the vectors chapter, and it will give you a quick test for whether two vectors are perpendicular. In the next chapter, you will graph parallel and perpendicular lines and find their equations.

Congruence

2.1 Rigid Transformations

Look at this picture of two geometric figures.



They are the same shape, right? If you cut one out with scissors, it would lay perfectly on top of the other. In geometry, we say they are *congruent*.

What is the official definition of “congruent”? Two geometric figures are congruent if you can transform one into the other using only rigid transformations. You might be wondering now, what are rigid transformations? A transformation is *Rigid* if it does not change the distances between the points or the measure of the angles between the lines they form. The following are all rigid transformations:

- Translations
- Rotations
- Reflections

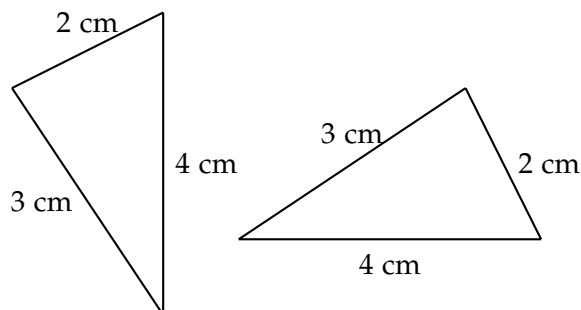
Once again, imagine cutting out one figure with scissors and trying to match it with the second figure; your actions are rigid transformations:

- Translations - Sliding the cutout left and right and up and down
- Rotations - Rotating the cutout clockwise and counterclockwise
- Reflection - Flipping the piece of paper over

A transformation is rigid if it is some combination of translations, rotations, or reflections.

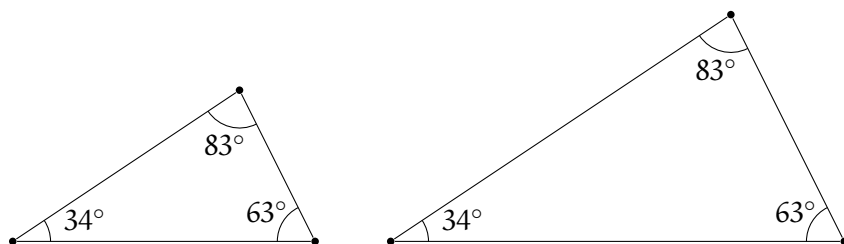
2.2 Triangle Congruency

If the sides of two triangles have the same length, the triangles must be congruent:



To be precise, the Side-Side-Side Congruency Test says that two triangles are congruent if three sides in one triangle are the same length as the corresponding sides in the other. We usually refer to this as the SSS test.

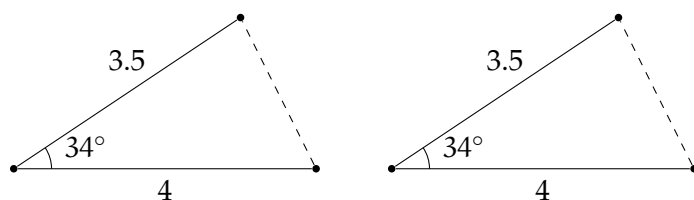
Note that two triangles with all three angles equal are not necessarily congruent. For example, here are two triangles with the same interior angles, but they are different sizes:



These triangles are not congruent, but they are *similar*. Meaning they have the same shape, but are not necessarily the same size.

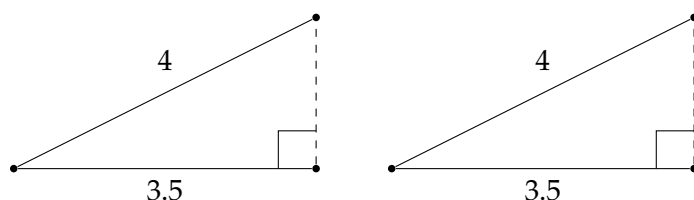
Since a triangle's angles always add up to 180° , knowing two angles tells you the third. This is why it makes sense to say "If two triangles have two angles that are equal, they are similar triangles." And if two similar triangles have one side that is equal in length, they must be the same size — so they are congruent. Thus, the Side-Angle-Angle Congruency Test says that two triangles are congruent if two angles and one side match.

What if you know that two triangles have two sides that are the same length, and that the angle between them is also equal?



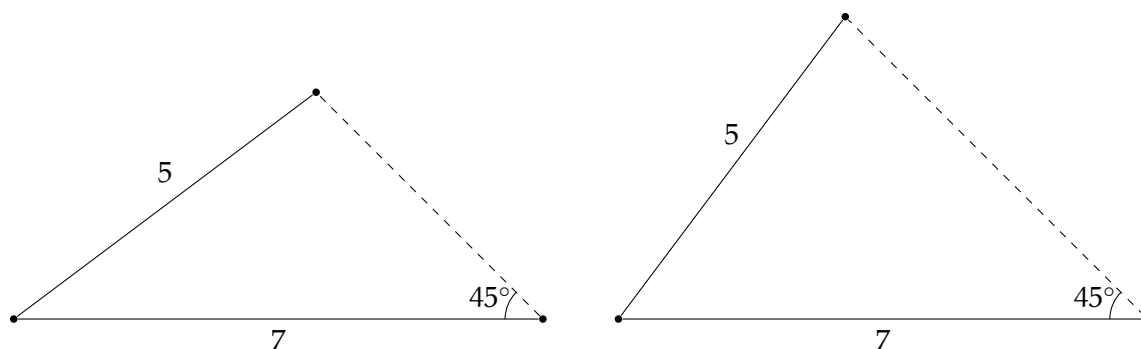
Yes, they must be congruent. This is the Side-Angle-Side Congruency Test.

What if the angle is not the one between the two known sides? If it is a right angle, you can be certain the two triangles are congruent. (How do we know? Because the Pythagorean Theorem tells us that we can calculate the length of the third side. There is only one possibility, so all three sides must be the same length.)

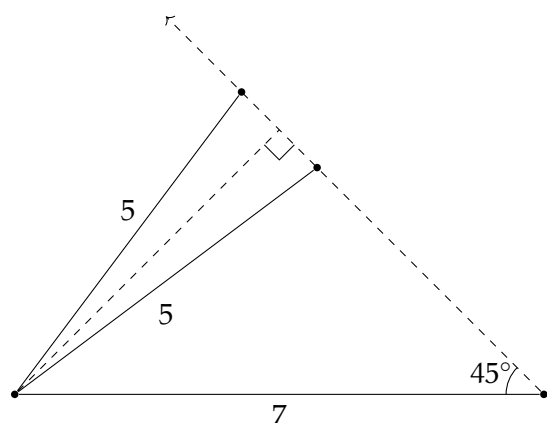


In this case, the third side of each triangle must be $\sqrt{4^2 - 3.5^2} \approx 1.9$.

What if the known angle is less than 90° ? *The triangles are not necessarily congruent.* For example, let us say that there are two triangles with sides of length 5 and 7 and that the corresponding angle (at the end of the side of length 7) on each is 45° . Two different triangles satisfy this:



Let us look at this another way by laying one triangle on top of the other:



This is why there is *not* a general Side-Side-Angle Congruency Test.

Here, then, is the list of common congruency tests:

- Side-Side-Side: All three sides have the same measure
- Side-Angle-Angle: Two angles and one side have the same measure
- Side-Angle-Side: Two sides and the angle between them have the same measure
- Side-Side-Right: They are right triangles and have two sides the same measure (often called Hypotenuse-Leg, or HL)

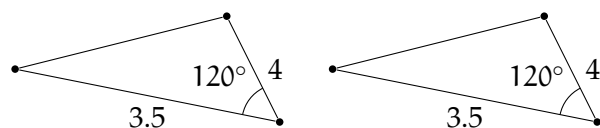
Worked example: SAS congruence. Triangle ABC has $AB = 4$, $BC = 5$, and $\angle B = 50^\circ$. Triangle DEF has $DE = 4$, $EF = 5$, and $\angle E = 50^\circ$. Two sides and the angle between them match, so the triangles are congruent by SAS. Therefore $AC = DF$, and every pair of matching angles is equal.

Once you know two triangles are congruent, you know *everything* matches: all three sides and all three angles. This is called CPCTC, short for “corresponding parts of congruent triangles are congruent.” It is how proofs in geometry usually finish.

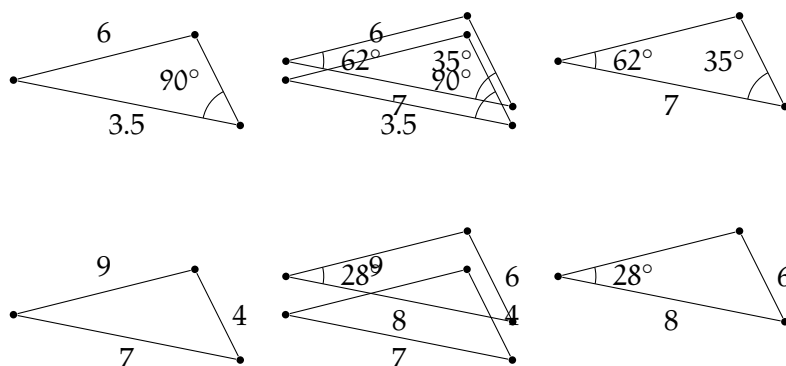
Exercise 6 Congruent Triangles

Ted is terrible at drawing triangles; he always draws them exactly the same. Fortunately, he has marked these diagrams with the sides and angles that he measured. For each pair of triangles, write whether you know them to be congruent and which congruency test proves it. For example:

Working Space



(These drawings are clearly not accurate, but you are told the measurements are.)
The answer is "Congruent by the Side-Angle-Side test."



Answer on Page 88

Exercise 7 Sides in Proportion

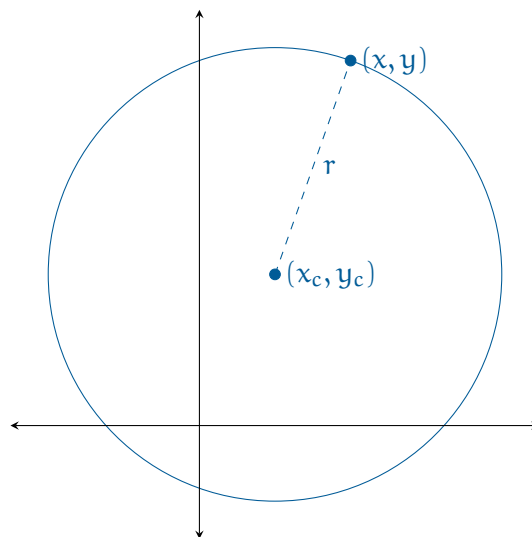
Triangles have sides 3, 4, 5 and 6, 8, 10.
Are they congruent? Explain.

Working Space

Answer on Page 88

Circles

Pizzas, wheels, clock faces, the rim of a basketball hoop: circles are everywhere. Here is the precise definition. A circle is the set of points (x, y) that are a fixed distance r from a fixed point (x_c, y_c) . The distance r is the *radius*, and (x_c, y_c) is the *center*.



Area and Radius

If the radius of a circle is r , the area of its interior (a) is given by

$$a = \pi r^2$$

Exercise 8 Area of a Circle

Working Space

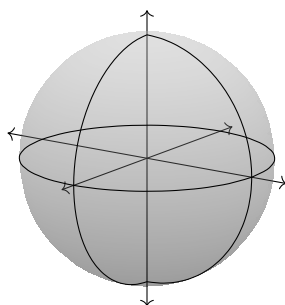
Your paint can says “One liter covers 6 square meters.”

You are painting the top of a circular table with a radius of 3 meters.

How much paint will you need?

Answer on Page 88

A circle lives in a plane. In 3D, the points (x, y, z) that are a fixed distance r from a fixed point (x_c, y_c, z_c) form a sphere:



The distance straight across a circle (or a sphere), through the center, is its *diameter*. The diameter is always twice the radius.

For the rest of the chapter, we stay *in a plane*: circles, points, and lines, all on a flat sheet of paper.

Circumference and Diameter

The circumference (c) of a circle is the distance around the circle. If the diameter is d ,

$$c = \pi d$$

Exercise 9 Circumference

Working Space

You wrap a tape measure around a tree in your yard. Its circumference is 64 cm. Assuming the trunk is roughly circular,

what is its diameter?

Answer on Page 89

Exercise 10 Splitting a Pie

Working Space

A pie has a radius of 13 cm. Seven friends all want equal slices, and you have a tape measure. How long should the outer crust of each slice be?

Answer on Page 89

3.1 Arc Length

You have already measured angles in degrees and in radians. A full trip around a circle is 360° (see figure 3.1).

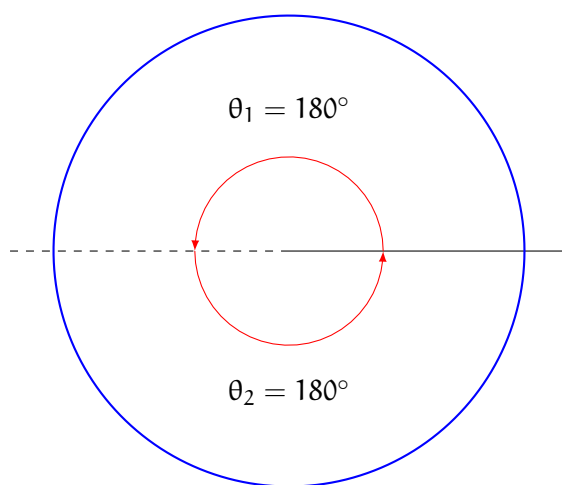


Figure 3.1: The total internal angle of a circle is $\theta_1 + \theta_2 = 360^\circ$

That is the same as 2π radians:

$$360^\circ \cdot \frac{\pi}{180^\circ} = 2\pi$$

But why π radians in 180° ? Because of how a radian is defined: one radian is the central angle that cuts off an arc exactly as long as the radius (see figure 3.2). Imagine bending a piece of string the length of the radius around the edge of the circle. The angle it spans is one radian.

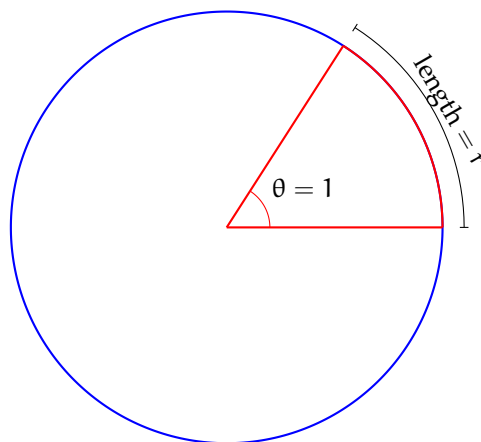
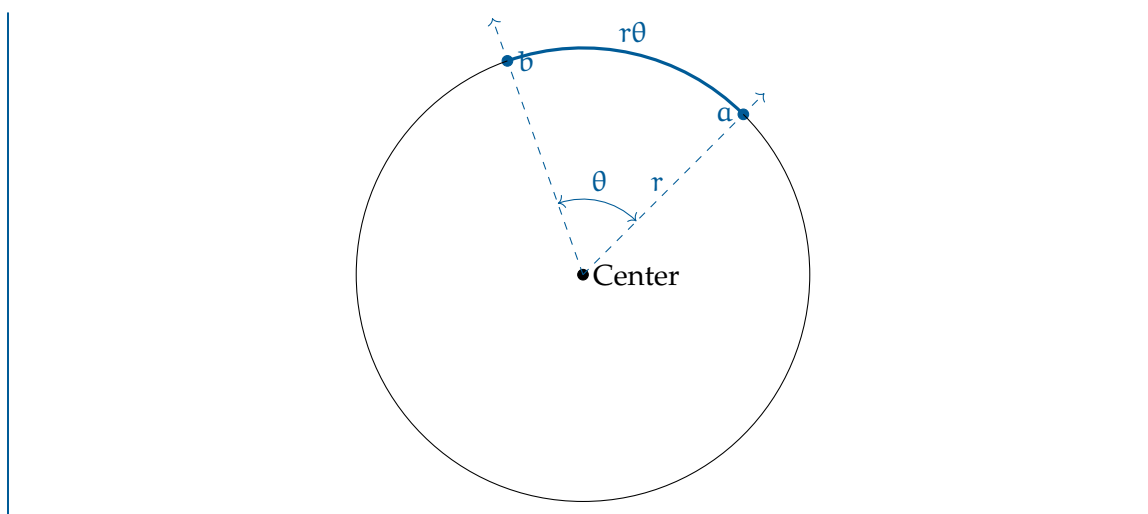


Figure 3.2: When the center angle is 1 radian, the length of the arc is equal to the radius of the circle

That definition makes arc length easy. Two radians of angle cut off two radii of arc, three radians cut off three, and so on. The arc length is just $r\theta$, with θ in radians.

Length of an Arc

If you have two points a and b on a circle, the ray from the center through a and the ray from the center through b form an angle. If θ is the angle in radians and r is the radius of the circle, the distance from a to b on the circle is $r\theta$.



Now we can see why π radians $= 180^\circ$. The circumference is $c = \pi d = 2\pi r$. It is also an arc: the one whose central angle goes all the way around. Set the two lengths equal:

$$2\pi r = r\theta$$

$$\theta = 2\pi$$

So $360^\circ = 2\pi$ radians, and half of that gives $180^\circ = \pi$ radians.

Exercise 11 Angle of Rotation

A car tire has a radius of about 25 centimeters. If you roll the car forward 10 cm, through how many radians does the tire turn?

Working Space

Answer on Page 89

Exercise 12 Arc Length Ranking

Rank these arcs from longest to shortest. Each is given by its central angle and the radius of its circle.

1. central angle of $\frac{\pi}{4}$ and a radius of 2 cm

Working Space

2. central angle of π and a radius of 1 cm
3. central angle of $\frac{\pi}{10}$ and a radius of 5 cm
4. central angle of $\frac{3\pi}{4}$ and a radius of 3 cm

Answer on Page 89

Exercise 13 Arc Length

Working Space

You need the radius of a huge cylindrical tank. Your tape measure is only 15 meters long and does not reach around it.

You do have a compass, though. You hold one end of the tape against the tank and note which direction the wall faces there. Then you walk 15 meters along the wall and check the direction again.

You find that 15 meters represents 72 degrees of arc.

What is the radius of the tank in meters?

Answer on Page 90

3.2 Sector Area

You know the area of a whole circle: $A = \pi r^2$. What about one slice?

Example: A pizza with a radius of 18 cm is cut into 6 equal slices. What is the area of

each slice?

Solution: First, we find the area of the entire pizza:

$$A = \pi r^2$$

$$A = \pi(18 \text{ cm})^2$$

$$A = 324\pi \text{ cm}^2 \approx 1018 \text{ cm}^2$$

Then we divide by 6, since the slices are equal:

$$A_{\text{piece}} = \frac{A}{6} = \frac{324\pi \text{ cm}^2}{6} = 54\pi \text{ cm}^2$$

Now let us turn this into a formula for a *sector*, a slice with central angle θ (see figure 3.3). Each of the 6 slices has central angle $\theta = \frac{2\pi}{6} = \frac{\pi}{3}$, and its area is the total divided by 6: $A_{\text{sector}} = \frac{\pi r^2}{6} = \frac{\pi}{6} r^2 = \frac{\theta}{2} r^2$.

Area of a sector

For a sector whose corner is at the center of a circle, the area is given by $A_{\text{sector}} = \frac{\theta}{2} r^2$, where θ is the central angle and r is the radius.

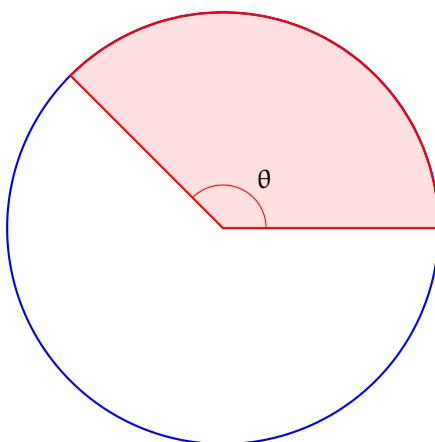


Figure 3.3: The area of a sector with central angle θ is $\frac{\theta}{2} r^2$

Exercise 14 Area of a sector

You are painting a circular logo, 5 meters wide, on the side of a building. One sector of the logo, with central angle $\frac{3\pi}{4}$

Working Space

radians, is red. If a liter of paint covers 6 square meters, how much red paint do you need?

Answer on Page 90

3.3 Secants and Tangents

A line that is *tangent* to a circle touches it at exactly one point, as shown in figure 3.4.

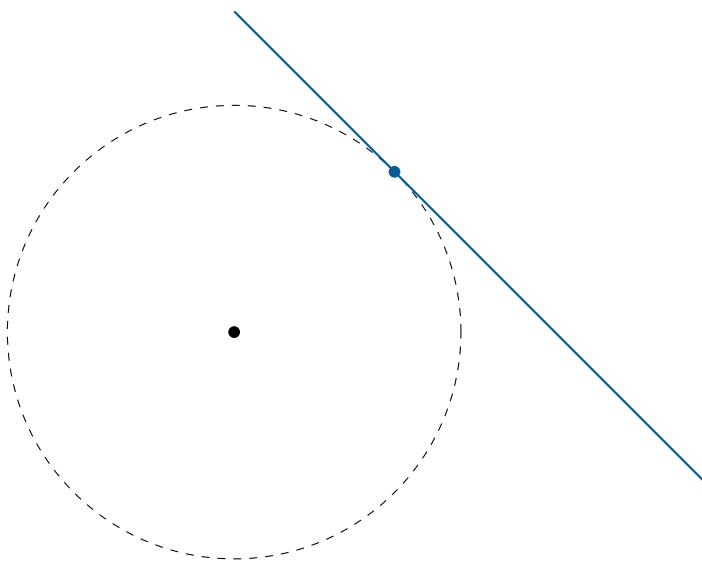


Figure 3.4: A line that is *tangent* to the circle.

The tangent line is always perpendicular to the radius to the point of tangency, as in figure 3.5.

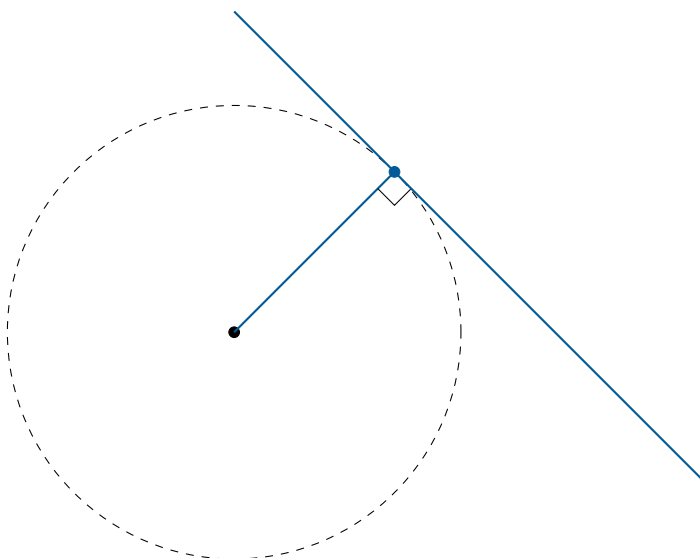


Figure 3.5: The radius and tangent line are perpendicular.

A secant line intersects a circle at *two points*, as shown in figure 3.6.

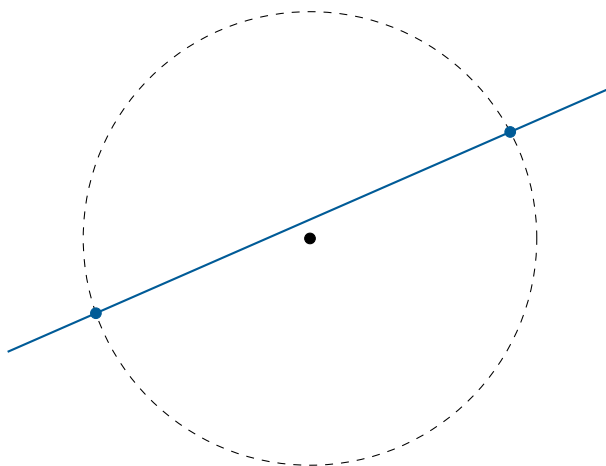


Figure 3.6: A line that is *secant* to the circle.

The piece of a secant line between its two crossing points is a *chord*. Every secant contains a chord, and every chord extends to a secant.

Remember these two words. In calculus, secant lines measure the average rate of change of a curve, and tangent lines measure its rate of change at a single instant.

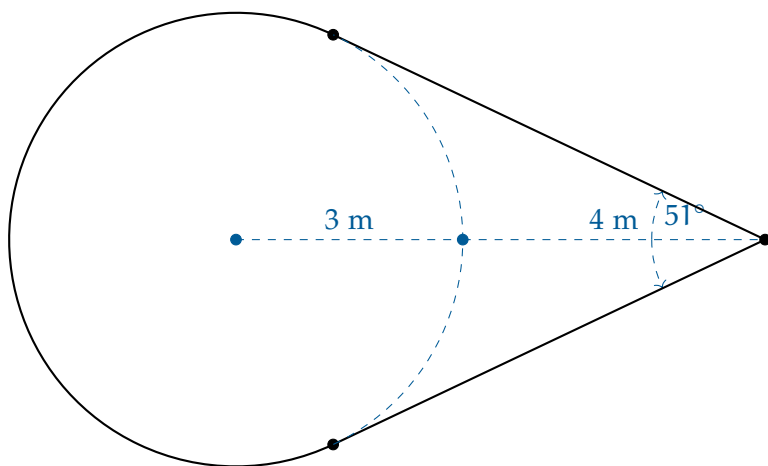
Exercise 15 **Painting a Comet***Working Space*

For the big game, you are painting a yellow comet on the gym floor.

A liter of yellow paint covers 6 square meters.

First you draw a circle with a radius of 3 meters. You then mark a point D on the floor 7 meters from the center of the circle. Then you draw two tangent lines that pass through D.

You use a protractor to measure the angle at which the tangent lines meet: about 51°



Before you paint the area contained by the circle and the two tangent lines, how much paint will you need?

Answer on Page 91

Functions and Their Graphs

Think of a vending machine. You press B4, and out comes the same bag of chips every time. A function works the same way: you put in a number, the function follows its rule, and out comes exactly one answer.

Just as we use x to stand for a number, we often use f to stand for a function. We write $f(x)$ and say “ f of x .” The name does not have to be f . Any letter or word will do, even $zebra(x)$.

For example, let the function f be defined like this:

$$f(x) = -5x^2 + 12x + 2$$

What is $f(3)$?

Run 3 through the machine: $-5(3^2) + 12(3) + 2 = -45 + 36 + 2 = -7$. So $f(3) = -7$.

Some functions refuse certain inputs. For example:

$$f(x) = \frac{1}{x}$$

This works for any x except 0, because you cannot divide by 0. The set of inputs a function accepts is its *domain*. The set of outputs it produces is its *range*.

A function gives exactly one output for each input. Two inputs may share an output (both 2 and -2 square to 4), but one input can never give two outputs. A rule that does give two outputs for some input is called a *relation*, not a function. The [vertical line test](#) spots these.

Exercise 16 Domain of a function

Working Space

Let the function f be given by
 $f(x) = \sqrt{x-3}$. What is its domain?

Answer on Page 92

Worked example: evaluating a function. Let $f(x) = x^2 - 1$. Then $f(3) = 9 - 1 = 8$, and $f(-2) = 4 - 1 = 3$.

4.1 Graphs of Functions

If you have a function, f , its graph is the set of pairs (x, y) such that $y = f(x)$. We usually draw a picture of this set, called a *graph*. The graph not only includes the picture, but also the values of x and y used to create it.

Here is the graph of the function $f(x) = -5x^2 + 12x + 2$:

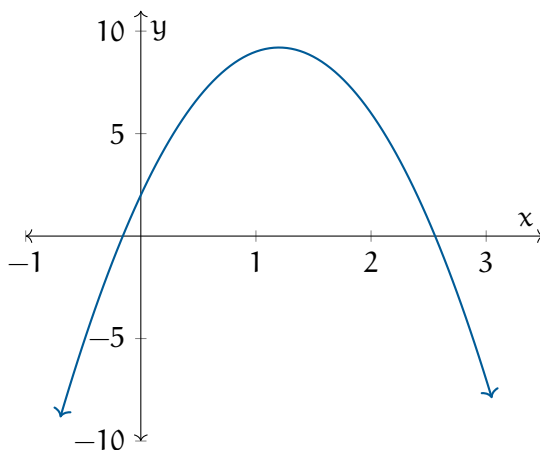


Figure 4.1: The function $f(x) = -5x^2 + 12x + 2$ *graphed* on an xy -plane from $x = -1$ to $x = 3$. The inputs x are graphed along the x -axis, and the output of the function $f(x)$ is plotted along the y -axis.

This is just part of the graph. The curve keeps going down forever on both sides; we only drew the interesting middle.

Here is the graph of the function $f(x) = \frac{1}{x}$:

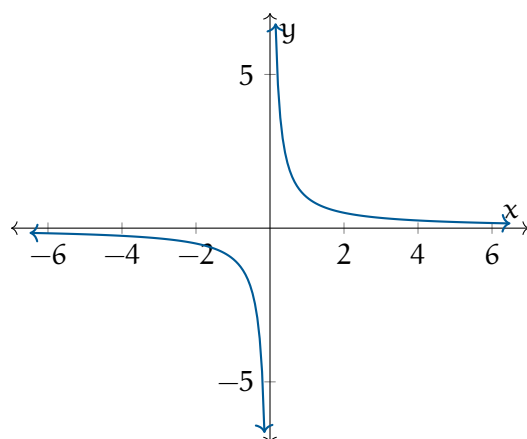


Figure 4.2: The function $f(x) = \frac{1}{x}$ graphed on a coordinate plane.

Notice the *asymptotes*, the lines $x = 0$ and $y = 0$. The curve gets closer and closer to them but never touches. It cannot touch $x = 0$ because $f(0)$ is undefined. It cannot touch $y = 0$ because $\frac{1}{x}$ is never zero: as x grows, $\frac{1}{x}$ shrinks toward 0 without ever arriving. You will see much more of asymptotes in the rational functions chapter.

To draw a graph by hand, pick several x values, compute $f(x)$ for each, plot the points $(x, f(x))$, and connect them smoothly.

Exercise 17 Draw a graph

Working Space

Let the function f be given by
 $f(x) = -3x + 3$. Sketch its graph.

Answer on Page 92

4.2 Can this be expressed as a function?

Not every set of points is the graph of a function. Here is the set of points (x, y) with $x^2 + y^2 = 9$:

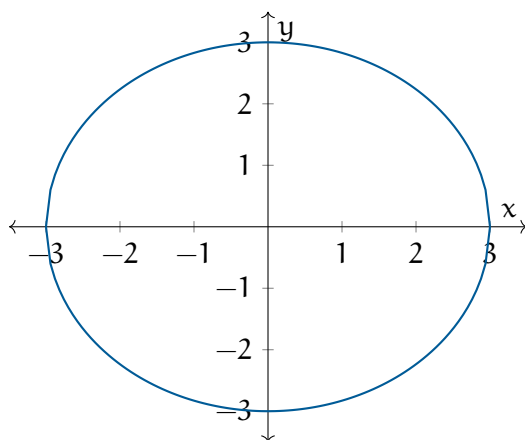


Figure 4.4: The graph of $x^2 + y^2 = 9$.

This circle cannot be the graph of a function. What would $f(0)$ be: 3 or -3 ? It fails the *vertical line test*: if any vertical line hits a set in more than one point, the set is not the graph of a function. For example, the vertical line $x = 2$ would cross the graph twice:

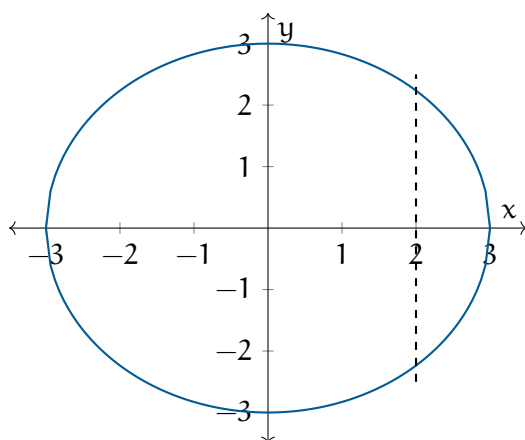


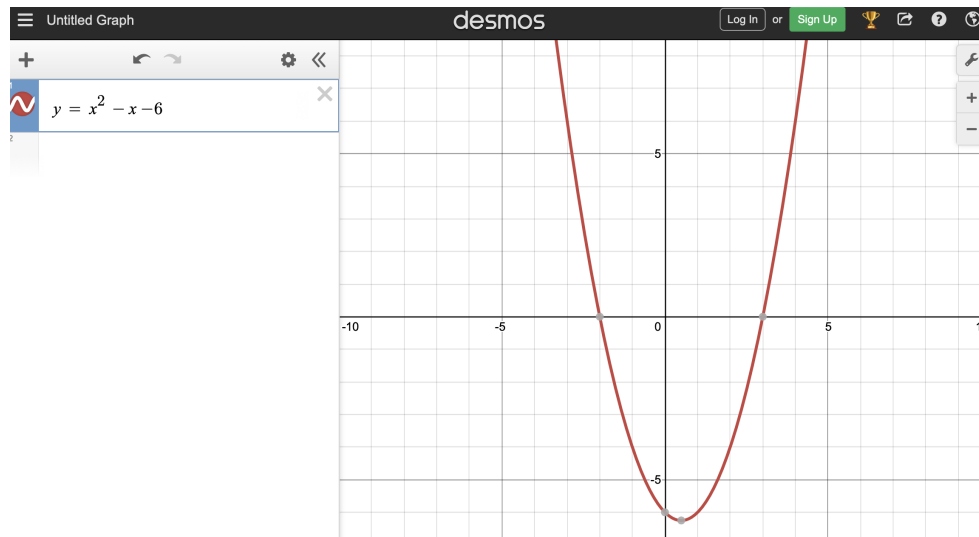
Figure 4.5: Vertical line test on $x^2 + y^2 = 9$.

4.3 Graphing Calculators

The fastest way to see a function is a graphing calculator. Desmos is a free one that runs in your browser.

In a web browser, go to Desmos: <https://www.desmos.com/calculator>

In the field on the left, enter the function $y = x^2 - x - 6$. (For the exponent, just prefix it with a caret symbol: "x^2".)



Computing in Python

Python can draw the same graph. The listing below uses two libraries: NumPy, which builds lists of numbers called *arrays*, and Matplotlib, which plots them.

```

1 import numpy as np
2 import matplotlib.pyplot as plt
3
4 def f(x):
5     return x**2 - x - 6
6
7 x = np.linspace(-5, 6, 200)
8 y = f(x)
9
10 plt.plot(x, y)
11 plt.axhline(0, color="black", linewidth=0.8)
12 plt.axvline(0, color="black", linewidth=0.8)
13 plt.grid(True)
14 plt.xlabel("x")
15 plt.ylabel("y")
16 plt.title("y = x^2 - x - 6")
17 plt.show()
```

The `def` line packages the rule $x^2 - x - 6$ into a Python function named `f`. Calling `f(3)` runs 3 through the machine, the same way `f(3)` does on paper. The call `np.linspace(-5, 6, 200)` creates 200 evenly spaced `x` values from `-5` to `6`, and passing that whole array

to `f` returns the 200 matching `y` values at once. Matplotlib then draws a point at each (x, y) pair and joins neighboring points with short line segments. With 200 points, each segment is short enough that the curve looks smooth. The calls `axhline` and `axvline` draw the x -axis and y -axis, and `plt.show()` opens the plot window.

Exercise 18 Reading values from `f`

Add this line after the plot code:

Working Space

```
1 print(f(0), f(3), f(-2))
```

What does it print? What do the three outputs tell you about the graph?

Answer on Page 92

Desmos handles the asymptote of $\frac{1}{x}$ on its own. Matplotlib joins every pair of neighboring points, so the two branches of $\frac{1}{x}$ need separate arrays, one on each side of $x = 0$:

```
1 x_left = np.linspace(-6, -0.15, 100)
2 x_right = np.linspace(0.15, 6, 100)
3
4 plt.plot(x_left, 1 / x_left, color="C0")
5 plt.plot(x_right, 1 / x_right, color="C0")
6 plt.axhline(0, color="black", linewidth=0.8)
7 plt.axvline(0, color="black", linewidth=0.8)
8 plt.ylim(-7, 7)
9 plt.grid(True)
10 plt.title("y = 1/x")
11 plt.show()
```

Both calls use `color="C0"`, Matplotlib's default blue, so the two branches read as one function. The call `plt.ylim(-7, 7)` fixes the visible y range to match Figure 4.2.

Exercise 19 The phantom line

A student plots $\frac{1}{x}$ with a single array:

Working Space

```
1 x = np.linspace(-6, 6, 100)
```

```

2 plt.plot(x, 1 / x)
3 plt.show()

```

The graph shows a vertical line running up the y-axis. The function has no value at $x = 0$. Where does the line come from?

Answer on Page 93

4.4 Even and Odd Functions

4.4.1 Even Functions

An even function is symmetric about the y-axis: fold the graph along the y-axis, and the two sides match perfectly. In other words, x and $-x$ always give the same output.

Even Functions

A function $f(x)$ is even if

$$f(-x) = f(x)$$

for all x in its domain.

Examples:

- $f(x) = x^2$
- $f(x) = \cos(x)$
- any $f(x) = x^n$ where n is an even number
- $f(x) = |x|$

4.4.2 Odd Functions

An odd function is symmetric about the origin: spin the graph 180° around the origin, and it lands on itself. In other words, if k goes in and n comes out, then $-k$ goes in and $-n$ comes out.

Odd Functions

A function $f(x)$ is odd if

$$f(-x) = -f(x)$$

for all x in its domain.

Equivalently,

$$f(x) + f(-x) = 0$$

for all x in its domain.

- $f(x) = x^3$
- $f(x) = \sin(x)$
- $f(x) = \tan(x)$
- any $f(x) = x^n$ where n is an odd number

4.4.3 Neither Even Nor Odd

Some functions are neither even nor odd.

For example, $f(x) = x^3 + 1$ satisfies neither condition: $f(1) = 2$, but $f(-1) = 0$, which is neither 2 nor -2 .

Computing in Python

A plot can test for symmetry. Draw $h(x)$, $h(-x)$, and $-h(-x)$ on one set of axes. When the $h(-x)$ curve lies on top of $h(x)$, the function is even. A match between $-h(-x)$ and $h(x)$ means the function is odd.

```

1 import numpy as np
2 import matplotlib.pyplot as plt
3
4 def h(x):
5     return x**3 + 1
6
7 x = np.linspace(-2, 2, 200)
8
9 plt.plot(x, h(x), label="h(x)")
10 plt.plot(x, h(-x), linestyle="--", label="h(-x)")
11 plt.plot(x, -h(-x), linestyle=":", label="-h(-x)")
12 plt.grid(True)
```

```

13 plt.legend()
14 plt.show()

```

Writing $h(-x)$ negates every entry of the array before it reaches h , and the extra minus sign in $-h(-x)$ negates every output afterward. For $h(x) = x^3 + 1$, the dashed and dotted curves both separate from the solid one, so $x^3 + 1$ is neither even nor odd.

The function `np.allclose(a, b)` turns the visual check into a yes or no answer. It returns **True** when two arrays agree at every entry, allowing for tiny rounding errors:

```

1 print(np.allclose(h(-x), h(x))) # even test
2 print(np.allclose(-h(-x), h(x))) # odd test

```

Both lines print **False** for $h(x) = x^3 + 1$.

Exercise 20 One input is enough

Predict the output, then run it:

Working Space

```

1 print(h(1), h(-1), -h(-1))

```

How do these three numbers show that h is neither even nor odd?

Answer on Page 93

Exercise 21 Swap the function

Change the body of `h` to `return np.abs(x)` and run the plot and both `allclose` tests. Then change it to `return x**3` and run everything again. For each version, which curve lands on top of the solid one, and what do the tests print?

Working Space

Answer on Page 93

4.5 Piecewise Functions

Your phone plan might charge one rate for the first few gigabytes and another after that. Rules like this are *piecewise functions*: they use different formulas on different parts of the domain. You pick the formula based on where the input falls. Here is a simple example:

$$f(x) = \begin{cases} \frac{1}{x} & x < 0 \\ x^2 & x \geq 0 \end{cases}$$

When $x < 0$, we use $\frac{1}{x}$; when $x \geq 0$, we use x^2 . The input $x = 0$ would break $\frac{1}{x}$, but it falls in the x^2 case, so f is defined for every real number. Here is a table of values:

x	-2	-1	0	0.1	1	2
$f(x)$	$-\frac{1}{2}$	-1	0	0.01	1	4

And here is the graph:

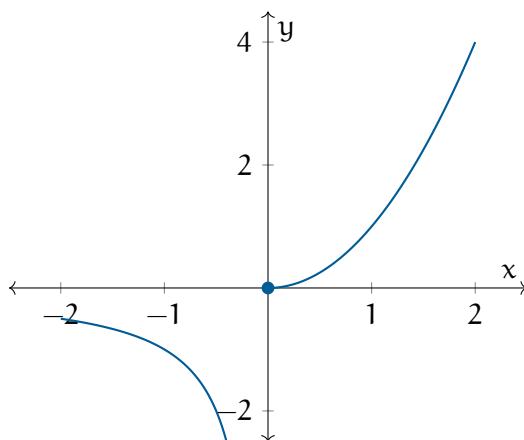
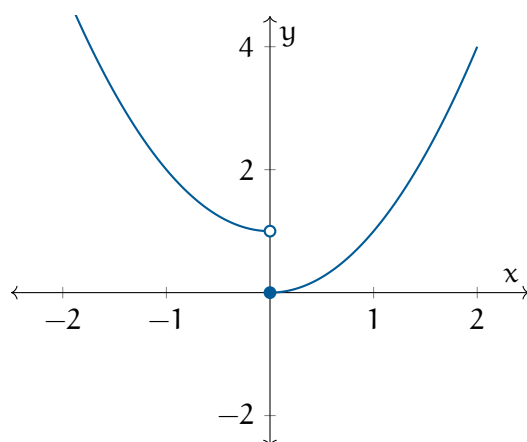


Figure 4.6: The piecewise function $f(x)$ graphed.

Notice the *closed circle* at $(0, 0)$. A closed circle marks a point that is on the graph. An *open circle* marks a point that is not. Here is a function that needs both:

$$g(x) = \begin{cases} x^2 + 1 & x < 0 \\ x^2 & x \geq 0 \end{cases}$$

Its graph has an open circle at $(0, 1)$, where the left piece stops just short, and a closed circle at $(0, 0)$, where the right piece starts.

Figure 4.7: The piecewise function $g(x)$ graphed.**Exercise 22** **Absolute Value***Working Space*

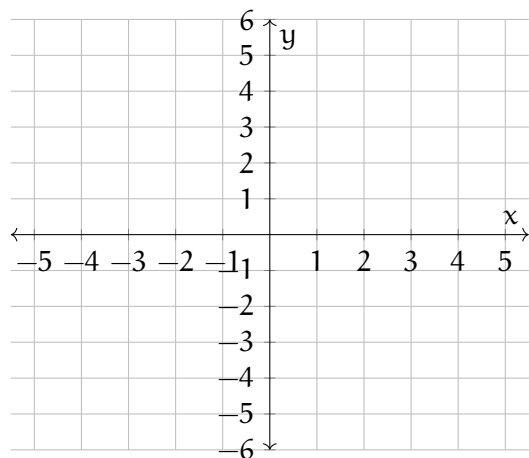
Rewrite the absolute value function $|x|$
as a piecewise function.

*Answer on Page 93***Exercise 23** **Piecewise 1***Working Space*

$$f(x) = \begin{cases} x + 2 & \text{if } -5 \leq x < -1 \\ x^2 & \text{if } -1 \leq x \leq 2 \\ 3 - x & \text{if } 2 < x \leq 5 \end{cases}$$

Make a table of $f(x)$ for every integer from -5 to 5 , then graph f .

Here is a blank coordinate plane for plotting the piecewise function:



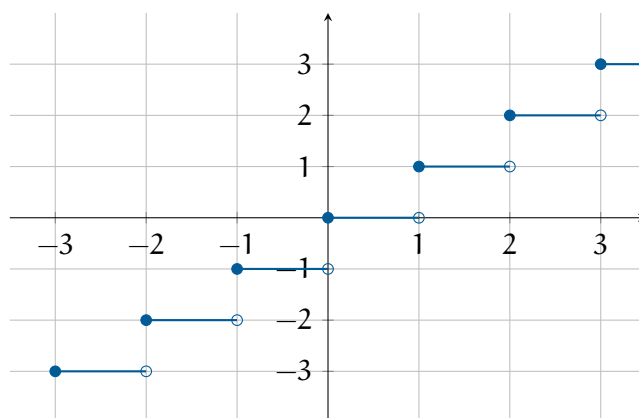
[Answer on Page 93](#)

4.5.1 Floor and Ceiling Functions

Two famous piecewise functions are the *floor function* and the *ceiling function*. The floor of any real number x is

$$\lfloor x \rfloor \text{ or } \text{floor}(x) = \begin{cases} n & \text{if } n \leq x < n+1, \quad n \in \mathbb{Z} \end{cases}$$

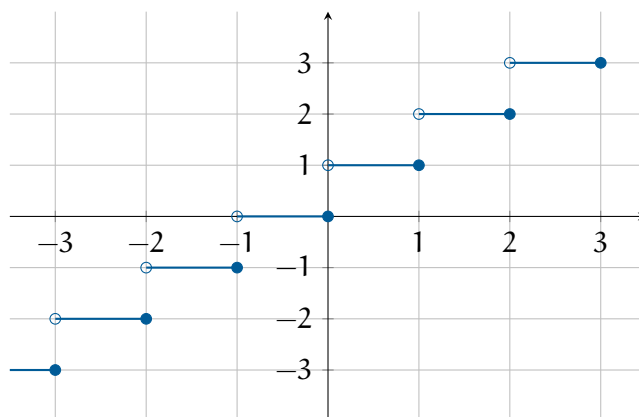
In words: the floor is the greatest integer less than or equal to x . For example, $\lfloor 0.7 \rfloor = 0$. Your age works this way: if you are 15.8 years old, you say you are 15.

Figure 4.8: The floor function, $f(x) = \lfloor x \rfloor$.

The ceiling function rounds the other way:

$$\lceil x \rceil \text{ or } \text{ceil}(x) = \begin{cases} n & \text{if } n-1 < x \leq n, \quad n \in \mathbb{Z} \end{cases}$$

The ceiling is the smallest integer greater than or equal to x . For example, $\lceil 8.00001 \rceil = 9$. Parking garages work this way: stay 2 hours and 1 minute, and you pay for 3 hours. For an integer such as 7, $\lfloor 7 \rfloor$ and $\lceil 7 \rceil$ are both 7.

Figure 4.9: The ceiling function, $f(x) = \lceil x \rceil$.

Exercise 24 More TVs is Better

Working Space

A store sells televisions with pricing that depends on how many units a customer buys:

- For the first 5 TVs, the cost per TV is \$400
- For the next 10 TVs, the cost per TV is \$350
- Any additional TVs cost \$300

A hotel is buying TVs for each hotel room.

1. Construct a piecewise function $C(x)$ for the cost of TVs. Assume TVs must be a discrete integer (you cannot buy 8.5 TVs).
2. Find the cost of 12 TVs using your function.
3. How many TVs must the hotel buy for the average cost per TV to drop below \$360?

Answer on Page 94

4.5.2 Invalid Piecewise Functions

When you write a piecewise function, make sure the cases do not overlap with different answers. Here is a broken one:

$$f(x) = \begin{cases} 10.2 & x = 4 \\ x^2 & x \geq 0 \end{cases}$$

At $x = 4$, the first case says $f(4) = 10.2$ and the second says $f(4) = 16$. One input, two outputs: not a function. The fix is to exclude 4 from the second case:

$$f(x) = \begin{cases} 10.2 & x = 4 \\ x^2 & x \geq 0, x \neq 4 \end{cases}$$

Now $f(4) = 10.2$, with no argument.

Computing in Python

Matplotlib draws a piecewise graph one piece at a time. Here is $g(x)$ from earlier in this section, with its open and closed circles:

```

1 import math
2 import numpy as np
3 import matplotlib.pyplot as plt
4
5 x_left = np.linspace(-2, 0, 100)
6 x_right = np.linspace(0, 2, 100)
7
8 plt.plot(x_left, x_left**2 + 1, color="C0")
9 plt.plot(x_right, x_right**2, color="C0")
10 plt.plot(0, 0, "o", color="C0") # closed circle
11 plt.plot(0, 1, "o", color="C0", markerfacecolor="white") # open circle
12 plt.grid(True)
13 plt.title("piecewise g(x)")
14 plt.show()

```

Each piece gets its own array covering only its part of the domain. A single array across the whole domain would join the two pieces with a vertical segment at $x = 0$, the same phantom line that appears with $\frac{1}{x}$. The format string "o" draws one round marker, and `markerfacecolor="white"` hollows it out into an open circle.

Plotting shows the shape. Evaluating the function at a particular input takes `if` and `elif`, with one condition for each row of the cases. This is the function from Exercise 23:

```

1 def p(x):
2     if -5 <= x < -1:
3         return x + 2
4     elif -1 <= x <= 2:
5         return x**2
6     elif 2 < x <= 5:
7         return 3 - x
8     return None
9
10 for x in range(-5, 6):
11     print(x, p(x))

```

Python accepts chained comparisons such as $-5 \leq x < -1$, written exactly in math notation. It checks the conditions from top to bottom and returns from the first one that is true. An input outside every case, such as $p(6)$, reaches the last line and returns `None`, Python's value for "nothing." That matches the function being undefined there. The call `range(-5, 6)` produces the integers from -5 up to 5 ; the stop value 6 is left out.

Exercise 25 **Checking the table**

Run the loop above. Compare its output with the table in the answer to Exercise 23. Which case does Python use at $x = -1$ and at $x = 2$?

*Working Space**Answer on Page 95***Exercise 26** **The case that never runs**

A student codes the revised function from the end of this section:

Working Space

```
1 def q(x):  
2     if x >= 0:  
3         return x**2  
4     elif x == 4:  
5         return 10.2
```

The call `q(4)` returns 16 instead of 10.2. Find the error and fix it.

*Answer on Page 95***Exercise 27** **Floor and ceiling in Python**

Python's `math` module provides `math.floor` and `math.ceil`. Predict the output:

Working Space

```
1 print(math.floor(-2.5), math.ceil(-2.5),  
    ↪ math.ceil(8.00001), math.floor(7))
```

Answer on Page 95

4.6 Summary

A function is a machine that turns each input into exactly one output. Its domain is the set of inputs it accepts; its range is the set of outputs it produces.

The graph of f is the set of points $(x, f(x))$. A set of points is the graph of a function only if it passes the vertical line test.

Even functions are mirror images across the y -axis ($f(-x) = f(x)$). Odd functions survive a half turn about the origin ($f(-x) = -f(x)$). Piecewise functions use different formulas on different parts of the domain; floor and ceiling are two famous examples.

Exercise 28 Solve for x

Let $g(x) = 2x + 5$. Find $g(-1)$, and find the value of x for which $g(x) = 11$.

Working Space

Answer on Page 96

Inverses and Transformations

5.1 Inverses

Put on your socks, then your shoes. To undo that, you take off your shoes, then your socks. Undoing is a big idea in math, and for functions it is called the inverse.

If a function f is a machine that turns x into y , its *inverse*, written f^{-1} , is the machine that turns y back into x .

For example, let $f(x) = 5x + 1$. The rule is “multiply by 5, then add 1.” To undo it, subtract 1, then divide by 5: $f^{-1}(x) = (x - 1)/5$. Spot check: $f(3) = 16$ and $f^{-1}(16) = 3$.

Does $f(x) = x^3$ have an inverse? Yes: $f^{-1}(x) = \sqrt[3]{x}$. Here is the function (solid) and its inverse (dashed):

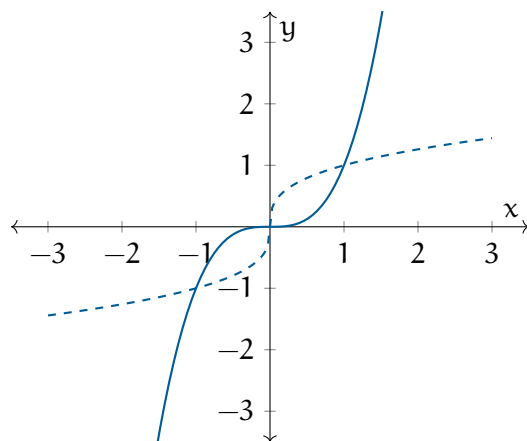


Figure 5.1: The function $f(x) = x^3$ and its inverse.

The inverse is the same curve with the axes swapped: every point (a, b) on f becomes (b, a) on f^{-1} . Swapping coordinates *reflects* the graph across the line $y = x$.

That gives a recipe for finding an inverse: swap x and y , then solve for y .

Worked example. Find the inverse of $f(x) = 2x + 1$.

Solution. Write $y = 2x + 1$ and swap: $x = 2y + 1$. Solve for y : $y = \frac{x-1}{2}$. So $f^{-1}(x) = \frac{x-1}{2}$. Check: $f(f^{-1}(x)) = 2\left(\frac{x-1}{2}\right) + 1 = x$. The inverse undoes the function, just as it should.

Not every function has an inverse. Take $f(x) = x^2$: $f(2) = f(-2) = 4$. What would $f^{-1}(4)$ be, 2 or -2 ? There is no way to choose. This gives the *horizontal line test*: if any horizontal line hits a function's graph more than once, the function has no inverse. A function that passes is *one-to-one*: each output comes from exactly one input.

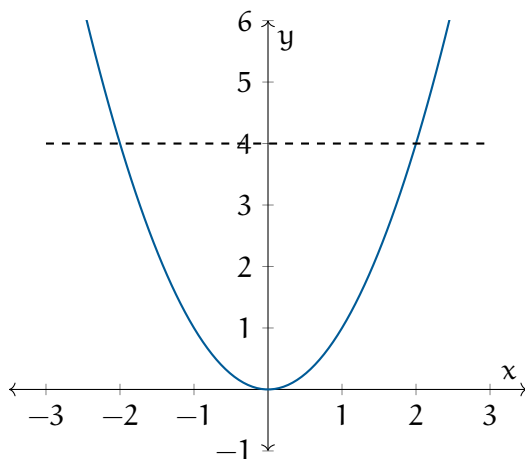


Figure 5.2: The horizontal line test run on $f(x) = x^2$.

Sometimes you can rescue an inverse by trimming the domain. If we keep only the non-negative inputs, $f(x) = x^2 - 5$ passes the horizontal line test, and its inverse is $f^{-1}(x) = \sqrt{x + 5}$.

What is the domain of f^{-1} ? Run every input in the domain of f through the machine and collect what comes out. That set is the *image*, or *range*, of f .

The range of $f(x) = x^2 - 5$ is the set of all real numbers greater than or equal to -5 . We write this:

$$\{x \in \mathbb{R} \mid x \geq -5\}$$

Now we can say: **The range (or image) of the function is the domain of the inverse function.**

The swap goes both ways: the domain of f is the range of f^{-1} . In our example, you can feed any number greater than or equal to -5 into f^{-1} .

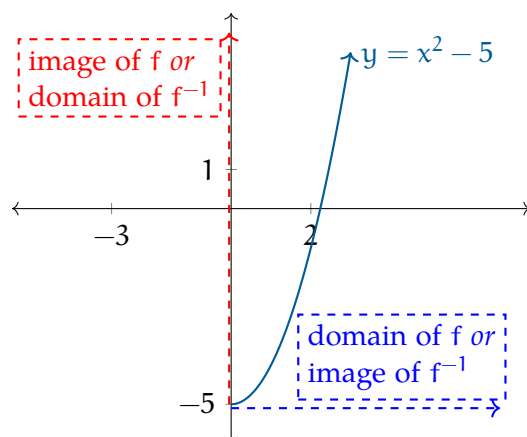


Figure 5.3: Domain and range of functions and their inverses get swapped.

Exercise 29 Find the inverse*Working Space*

Let $f(x) = (x-3)^2 + 2$. Sketch the graph.

Using all the real numbers as a domain, does this function have an inverse?

How would you restrict the domain to make the function invertible?

What is the inverse of that restricted function?

What is the domain of the inverse?

*Answer on Page 96***Exercise 30***Working Space*

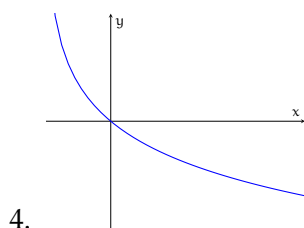
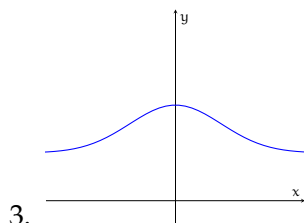
A function is given by a table of values, a graph, or a written description. Determine whether it is one-to-one. For the tables, assume the function changes smoothly between the listed points.

1.

x	1	2	3	4	5	6
$f(x)$	1.5	2.0	3.6	5.3	2.8	2.0

2.

x	1	2	3	4	5	6
$f(x)$	1.0	1.9	2.8	3.5	3.1	2.9



5. $f(t)$ is the height of a football t seconds after kickoff

6. $v(t)$ is the velocity of a dropped object

Answer on Page 96

Computing in Python

Figure 5.1 takes three plot calls: the function, its inverse, and the line $y = x$ that reflects one onto the other.

```

1  import numpy as np
2  import matplotlib.pyplot as plt
3
4  def g(x):
5      return x**3
6
7  def g_inv(x):
8      return np.cbrt(x)
9
10 x = np.linspace(-3, 3, 200)
11
12 plt.plot(x, g(x), label="g(x) = x^3")
13 plt.plot(x, g_inv(x), linestyle="--", label="inverse")

```

```
14 plt.plot(x, x, color="gray", linewidth=0.8, label="y = x")
15 plt.xlim(-3.5, 3.5)
16 plt.ylim(-3.5, 3.5)
17 plt.gca().set_aspect("equal")
18 plt.grid(True)
19 plt.legend()
20 plt.show()
```

The function `np.cbrt` returns the cube root of every entry in an array. Setting the aspect to `"equal"` gives one unit the same length on both axes. Without it, the window stretches one axis and the reflection across $y = x$ looks lopsided. The label strings feed `plt.legend()`, which prints the key in the corner.

Exercise 31 The missing half

Replace `np.cbrt(x)` with `x**(1/3)` and run the code again. The dashed curve now appears only to the right of the y-axis, and Python prints the warning `invalid value encountered in power`. Explain what happened.

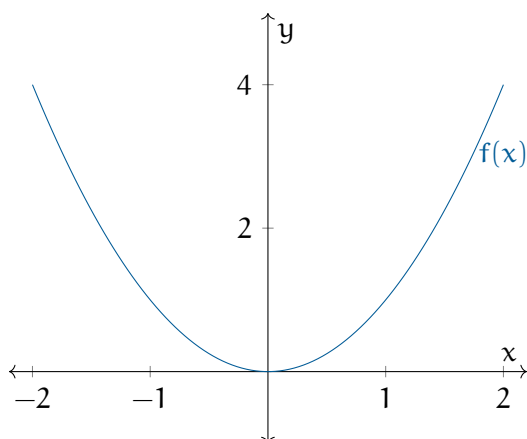
Working Space

Answer on Page 97

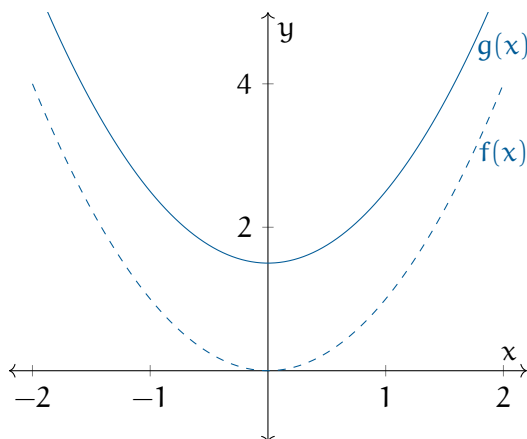
5.2 Transforming Functions

Remember sliding, flipping, and turning shapes in geometry? You can do the same to the graph of a function. Change the formula a little, and the graph moves in a predictable way.

Here is the graph of a function f :

Figure 5.5: A graph of x^2 .

Now let $g(x) = f(x) + 1.5$. Can you guess what the graph of g looks like? It is the same curve, lifted up 1.5:

Figure 5.6: $f(x)$ dashed and $g(x) = f(x) + 1.5$ solid.

Four transformations come up all the time:

- Translating up and down (the one you just saw)
- Translating left and right
- Stretching or squishing along the y axis
- Stretching or squishing along the x axis

We will show each one on the graph of $\sin(x)$, which you will meet properly in the trigonometry chapters. For now, just enjoy the wave.

5.2.1 Translation up and down

When you add a positive constant to a function, you translate the whole graph up that much. A negative constant translates it down.

Here is the graph of $\sin(x) - 0.5$:

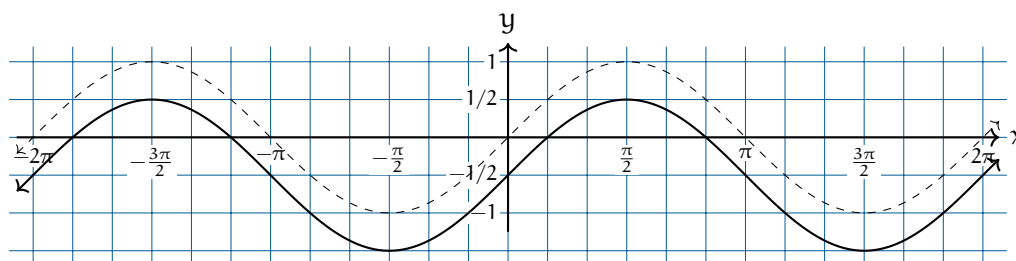


Figure 5.7: A graph of $\sin(x)$ dashed and $\sin(x) - 0.5$ in solid

5.2.2 Translation left and right

When you add a positive number to x before running it through f , the graph moves *left* by that amount. Subtracting moves it *right*. This feels backward at first. Here is why: $f(x+2)$ reaches any given output 2 units sooner than $f(x)$ does, so every feature arrives 2 units to the left.

Here is the graph of $\sin(x - \pi/6)$:

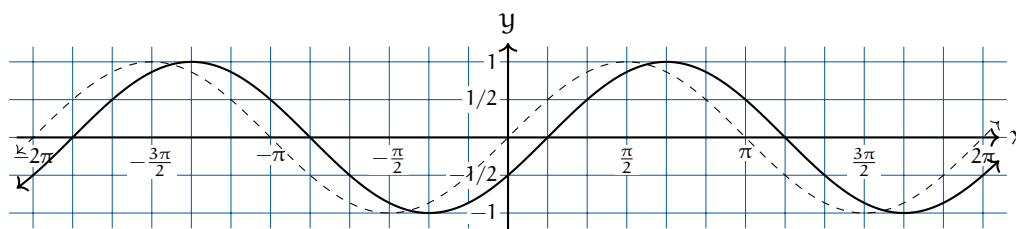


Figure 5.8: A graph of $\sin(x)$ in dashed lines and $\sin(x - \pi/6)$ in solid lines.

The solid curve sits $\frac{\pi}{6}$ to the right of the dashed one, even though the formula has a minus sign.

5.2.3 Scaling up and down in the y direction

To stretch a graph vertically, multiply the output by a constant. A constant larger than 1 stretches the graph taller; one between 0 and 1 squishes it flatter.

Here is $y = 2\sin(x)$:

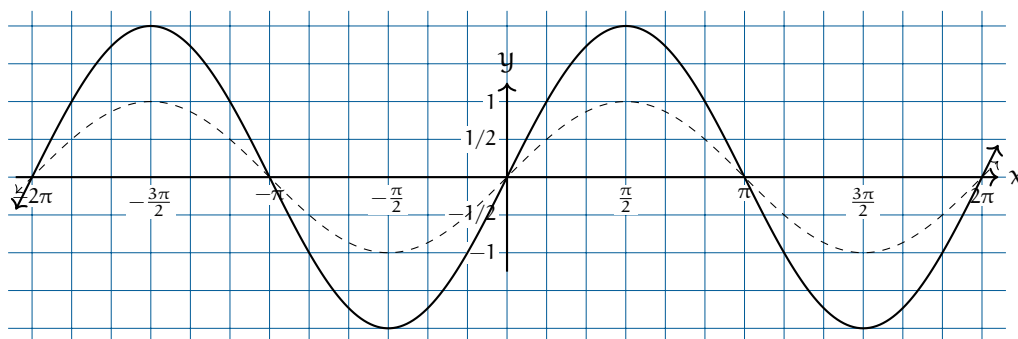


Figure 5.9: $\sin(x)$ dashed and $2\sin(x)$ solid.

A wave's *amplitude* is how far it swings from its baseline. This wave swings around 0, and multiplying by 2 raised its amplitude from 1 to 2.

Multiply by a negative number, and the graph flips upside down. Here is $y = -0.5\sin(x)$:

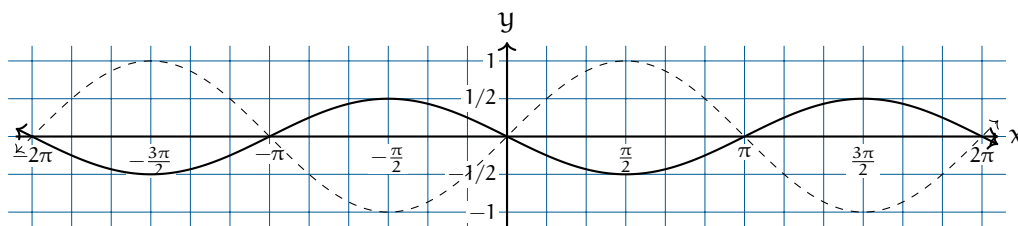


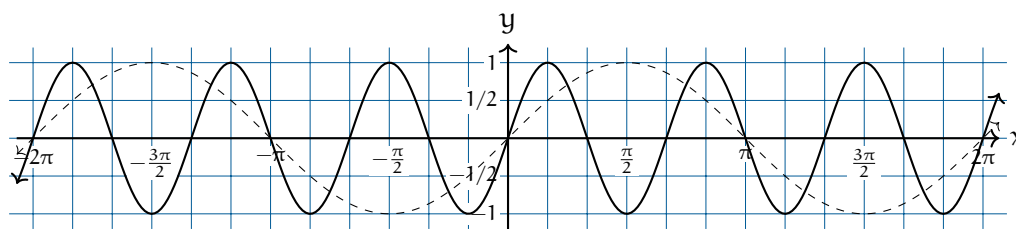
Figure 5.10: $\sin(x)$ dashed and $-0.5\sin(x)$ solid: squished and flipped.

Amplitude is a distance, so it is never negative. The amplitude of this wave is 0.5.

5.2.4 Scaling up and down in the x direction

Multiply x by a number larger than 1 before running it through the function, and the graph squishes toward the y axis. Everything happens sooner.

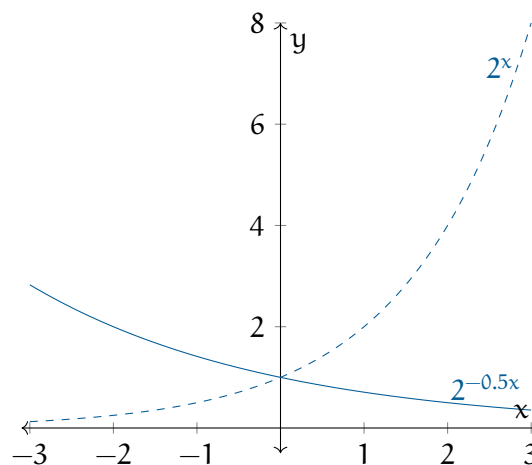
Here is $y = \sin(3x)$:

Figure 5.11: $\sin(x)$ dashed and $\sin(3x)$ solid.

The distance from one peak to the next is the *wavelength*. The original wave has wavelength 2π ; the squished wave has wavelength $\frac{2\pi}{3}$. Three waves now fit where one used to.

Multiply x by a number between 0 and 1, and the graph stretches away from the y axis. Multiply x by a negative number, and the graph flips across the y axis.

Here is $y = 2^{-0.5x}$. It is flipped across the y axis and stretched out along the x axis.

Figure 5.12: A base function 2^x in dashes compared to $2^{-0.5x}$ in solid.

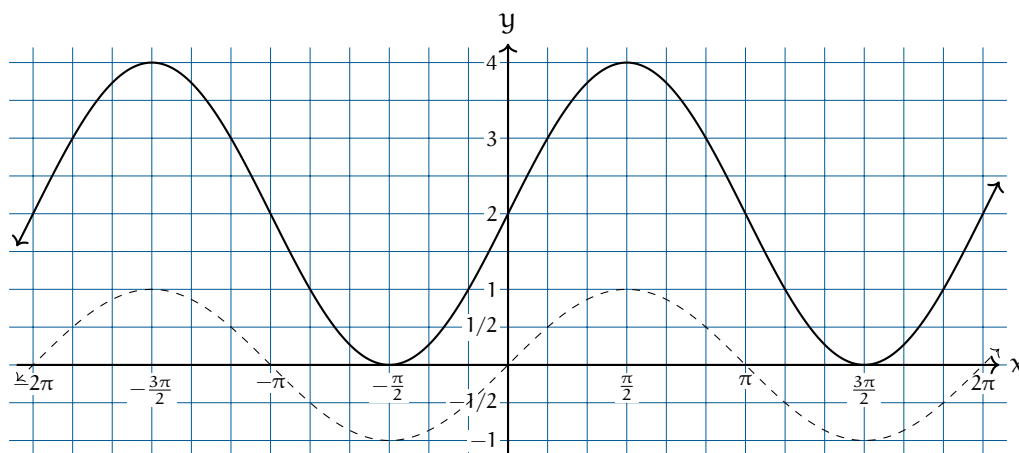
Reflection over x-axis	$(x, y) \rightarrow (x, -y)$
Reflection over y-axis	$(x, y) \rightarrow (-x, y)$
Translation	$(x, y) \rightarrow (x + a, y + b)$
Dilation	$(x, y) \rightarrow (kx, ky)$
Rotation 90° counterclockwise	$(x, y) \rightarrow (-y, x)$
Rotation 180°	$(x, y) \rightarrow (-x, -y)$

Figure 5.13: Where common transformations send a point (x, y) .

5.2.5 Order is important!

You can combine transformations. For example, you can translate a function up 1, then stretch it vertically by 2.

Here is $y = 2.0(\sin(x) + 1)$:

Figure 5.14: A graph of the base function $\sin(x)$ and the transformed function $2(\sin(x) + 1)$

A function is often a series of steps. Here are the steps in $f(x) = 2(\sin(x) + 1)$:

1. Take the sine of x
2. Add 1 to that
3. Multiply that by 2

Distributing the 2 gives the same function: $f(x) = 2\sin(x) + 2$.

What if we change the order? Here are the steps in $g(x) = 2\sin(x) + 1$:

1. Take the sine of x
2. Multiply that by 2
3. Add 1 to that

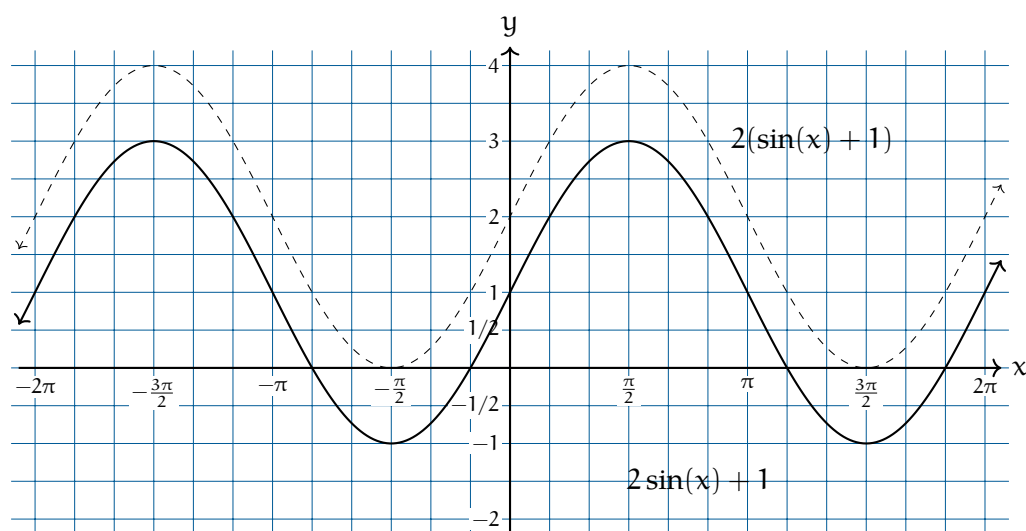


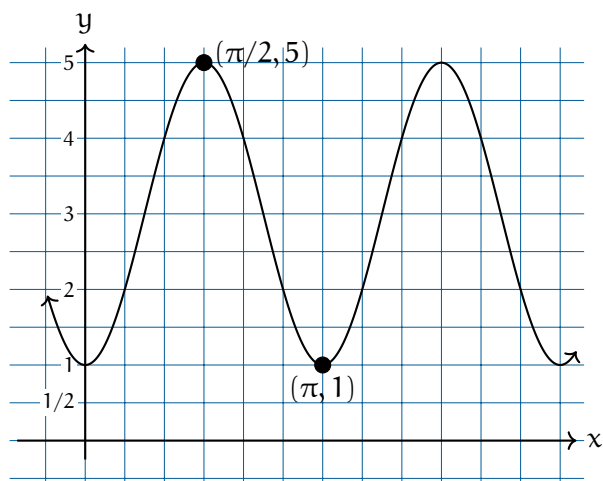
Figure 5.15: The functions $2\sin(x) + 1$ in solid compared to $2(\sin(x) + 1)$ in dashes.

The two curves differ by 1 everywhere. The moral: when you combine transformations, order matters. It is socks and shoes all over again.

Exercise 32 Transforms

Working Space

Find a function that creates a sine wave such that the top of the first crest is at the point $(\frac{\pi}{2}, 5)$ and the bottom of the trough that follows is at $(\pi, 1)$.



Answer on Page 97

5.2.6 Effects on even and odd Functions

Which transformations keep a function even or odd?

1. Vertical shifts ($f(x) + c$) keep an even function even: $x^2 + 1$ is still a mirror image across the y-axis. They break oddness: x^3 is odd, but $x^3 + 1$ is not.
2. Horizontal shifts ($f(x - c)$) usually break both. $\sin(x)$ is odd, but $\sin(x - \frac{\pi}{4})$ is neither. (Careful: $\sin(x - \frac{\pi}{2}) = -\cos(x)$, which happens to be even. Always check.)
3. Vertical stretches ($af(x)$) and horizontal stretches ($f(bx)$) keep the type: $3x^2$ is even, and $(2x)^3$ is odd.

When in doubt, compute $f(-x)$ and compare.

Exercise 33 Inverse of a Cube

Let $f(x) = x^3$. Find $f^{-1}(8)$.

Working Space

Answer on Page 98

CHAPTER 6

Solving Quadratics

Toss a ball, and its height follows a quadratic. So does the area of a square garden as you widen it, and the profit of a business as it raises prices. Sooner or later, you want to know *when* the ball lands or *which* price breaks even. That means solving a quadratic equation.

A *quadratic function* has the form $ax^2 + bx + c$. The numbers a , b , and c are its *coefficients*. They can be any constants, except that a cannot be zero. (If a is zero, the function is linear.)

Set a quadratic function equal to zero, and you have a *quadratic equation*. For example:

$$72x^2 - 12x + 1.2 = 0$$

How can you find the values of x that will make this equation true?

Dividing both sides by a never changes the solutions, so you can always make the first coefficient 1:

$$x^2 + bx + c = 0$$

For example, to solve $4x^2 + 8x - 19 = -2x^2 - 7$, move everything to the left side, then divide by 6:

$$4x^2 + 8x - 19 = -2x^2 - 7$$

$$6x^2 + 8x - 12 = 0$$

$$x^2 + \frac{4}{3}x - 2 = 0$$

Here, $b = \frac{4}{3}$ and $c = -2$.

6.1 Completing the Square

Some quadratics are easy. To solve $(x + 3)^2 = 16$, take the square root of both sides: $x + 3 = \pm 4$, so $x = 1$ or $x = -7$. (Do not forget the $\pm$: both 4^2 and $(-4)^2$ are 16.)

The trick is to make every quadratic look like that. Notice that

$$(x + 3)^2 = x^2 + 6x + 9$$

The middle coefficient, 6, is twice the 3, and the last term, 9, is 3^2 . So $x^2 + 6x$ is just 9 short of a perfect square. In general, $x^2 + bx$ is $(\frac{b}{2})^2$ short of the perfect square $(x + \frac{b}{2})^2$. Adding that missing piece is called *completing the square*.

Worked example. Solve $x^2 + 6x - 7 = 0$.

Solution. Move the -7 over: $x^2 + 6x = 7$. Half of 6 is 3, and $3^2 = 9$, so add 9 to both sides:

$$x^2 + 6x + 9 = 16$$

$$(x + 3)^2 = 16$$

$$x + 3 = \pm 4$$

So $x = 1$ or $x = -7$.

Now do the same thing with letters. Start with $x^2 + bx + c = 0$:

$$\begin{aligned} x^2 + bx &= -c \\ x^2 + bx + \frac{b^2}{4} &= \frac{b^2}{4} - c \\ \left(x + \frac{b}{2}\right)^2 &= \frac{b^2 - 4c}{4} \\ x + \frac{b}{2} &= \pm \frac{\sqrt{b^2 - 4c}}{2} \end{aligned}$$

That gives a formula that solves every quadratic whose first coefficient is 1:

When $a = 1$, $x^2 + bx + c = 0$ when

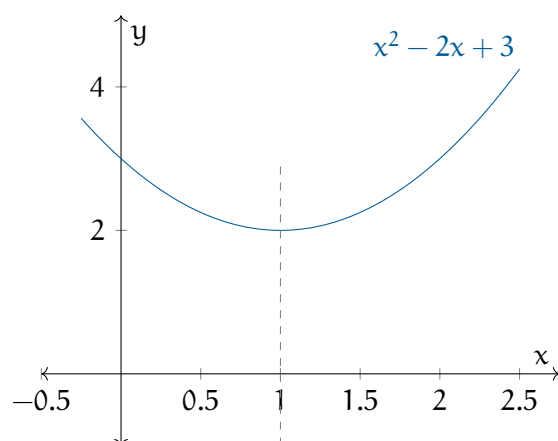
$$x = -\frac{b}{2} \pm \frac{\sqrt{b^2 - 4c}}{2}$$

Completing the square also tells you what the graph looks like. Since $x^2 + bx + c = (x + \frac{b}{2})^2 + (c - \frac{b^2}{4})$, the graph is a parabola that opens upward, and its lowest point, the vertex, is at $x = -\frac{b}{2}$, where the squared part is zero. For a quadratic with any value of a , the vertex is at $x = -\frac{b}{2a}$, which is called the vertex formula.

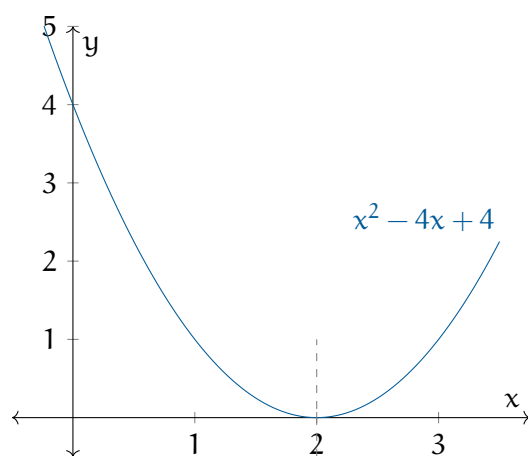
The number under the square root, $b^2 - 4c$, is called the *discriminant*. It tells you how many solutions (or *roots*) there are before you do any more work.

If $b^2 - 4c < 0$, there are no real roots. The parabola never gets low enough to reach the

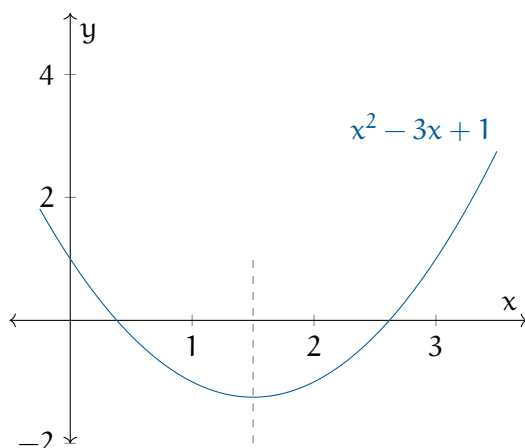
x-axis:



If $b^2 - 4c = 0$, there is one real root. The parabola just touches the x-axis at its vertex:



If $b^2 - 4c > 0$, there are two real roots. The parabola dips below the x-axis and comes back up, crossing it twice:



Exercise 34 Roots of a Quadratic

Working Space

You toss a hammer upward from a height of 2 meters at 12 m/s. Its height in meters after t seconds is

$$p = -\frac{1}{2}9.8t^2 + 12t + 2$$

When does the hammer hit the ground?

Answer on Page 98

6.2 The Traditional Quadratic Formula

Divide $ax^2 + bx + c = 0$ by a and complete the square, and you get the famous *quadratic formula*. It works directly, with no dividing first.

The Quadratic Formula

$ax^2 + bx + c = 0$ when

$$x = \frac{-b \pm \sqrt{b^2 - 4ac}}{2a}$$

This formula works for any quadratic equation, including ones where a is not 1. Recall the equation from the start of this chapter, $6x^2 + 8x - 12 = 0$. Here $a = 6$, $b = 8$, and $c = -12$. Substitute these into the formula:

$$x = \frac{-8 \pm \sqrt{8^2 - 4(6)(-12)}}{2(6)} = \frac{-8 \pm \sqrt{64 + 288}}{12} = \frac{-8 \pm \sqrt{352}}{12}$$

Since $\sqrt{352} \approx 18.762$, the $+$ gives $x \approx \frac{10.762}{12} \approx 0.897$, and the $-$ gives $x \approx \frac{-26.762}{12} \approx -2.230$.

Watch the signs. Since $c = -12$, the term $-4ac$ becomes $-4(6)(-12) = +288$, so the number under the square root grows.

Earlier, you divided this equation by 6 to get $x^2 + \frac{4}{3}x - 2 = 0$. The formula for $a = 1$ gives the same roots: with $b = \frac{4}{3}$ and $c = -2$, $-\frac{b}{2} \pm \frac{\sqrt{b^2 - 4c}}{2}$ also comes out to $x \approx 0.897$ and $x \approx -2.230$. Use whichever form is easier for the numbers in front of you.

The formula also answers the question at the start of this chapter. For $72x^2 - 12x + 1.2 = 0$, the number under the square root is $(-12)^2 - 4(72)(1.2) = 144 - 345.6 = -201.6$. No real number is the square root of a negative number, so this equation has no real solutions.

6.3 Factoring Quadratics

The quadratic formula always works, but the arithmetic can get heavy, especially without a calculator. For some quadratics, factoring is much faster.

Factoring rewrites a quadratic as a product of two simpler expressions. For example, $x^2 + 5x + 6$ can be written as $(x + 2)(x + 3)$. Expanding the product gives back the original: $x^2 + 3x + 2x + 6 = x^2 + 5x + 6$.

The factored form makes the roots easy to read because of the *zero product property*: if two numbers multiply to zero, at least one of them must be zero. So $(x + 2)(x + 3) = 0$ means $x + 2 = 0$ or $x + 3 = 0$, which gives $x = -2$ or $x = -3$. These are the same roots the quadratic formula gives, found without a square root.

Worked example. Solve $x^2 - 5x + 6 = 0$.

Solution. We need two numbers that multiply to 6 and add to -5 : -2 and -3 . So $(x - 2)(x - 3) = 0$, and $x = 2$ or $x = 3$. Check: $2^2 - 5(2) + 6 = 0$ and $3^2 - 5(3) + 6 = 0$.

Here are the factoring techniques worth knowing.

Types of Factoring Techniques

1. Factoring out the GCF (Greatest Common Factor)

Always check for a common factor first:

$$2x^2 + 4x = 2x(x + 2)$$

2. Factoring Trinomials: $a = 1$

For expressions like $x^2 + bx + c$, find two numbers that:

- Multiply to c
- Add to b

$$x^2 + 5x + 6 = (x + 2)(x + 3)$$

3. Factoring Trinomials: $a \neq 1$

Use the “AC method”:

- (a) Multiply $a \times c$
- (b) Find two numbers that multiply to ac and add to b
- (c) Split the middle term and factor by grouping

$$6x^2 + 11x + 4 = 6x^2 + 3x + 8x + 4 = 3x(2x + 1) + 4(2x + 1) = (3x + 4)(2x + 1)$$

4. Special Cases:

- Perfect Square Trinomials:

$$a^2 + 2ab + b^2 = (a + b)^2$$

$$x^2 + 6x + 9 = (x + 3)^2$$

- Difference of Squares:

$$a^2 - b^2 = (a - b)(a + b)$$

$$x^2 - 16 = (x - 4)(x + 4)$$

Tips

- Always factor out the GCF first.
- Check your result by expanding (FOIL). The inverse of factoring is expanding using the FOIL method.
- Some quadratics cannot be factored using integers. For those, use the quadratic formula.

Exercise 35 **Difference of Squares**

Solve $x^2 - 4 = 0$.

Working Space

Answer on Page 98

Exercise 36 **Pick your method**

Solve each equation. Choose factoring, completing the square, or the quadratic formula, whichever is easiest.

Working Space

1. $x^2 + 6x + 5 = 0$
2. $2x^2 + 7x + 3 = 0$
3. $x^2 - 10x + 18 = 0$
4. $x^2 + 2x + 5 = 0$

Answer on Page 98

Exercise 37 **Nothing but net**

You shoot a basketball from a height of 2 m. Its height after t seconds is $h = -4.9t^2 + 8t + 2$. The rim is 3.05 m high. At what times is the ball at rim height? Which one matters for making the shot?

Working Space

Answer on Page 99

Number Theory and Cryptography

Every time you log in to a website, your phone and a server you have never met agree on a secret, while anyone on the network can listen in. That sounds impossible. It works because of a few facts about whole numbers, some of them more than 2,000 years old. Multiplying two huge primes is easy; un-multiplying the result is so hard that no computer on Earth can do it in a lifetime. In this chapter, you will learn the number theory behind that idea and then use it to build *RSA*, the system that protected the internet for decades.

7.1 Divisibility

We say that a *divides* b , written $a \mid b$, if $b = ak$ for some integer k . Then a is a *divisor* (or *factor*) of b , and b is a *multiple* of a . For example, $3 \mid 12$ because $12 = 3 \cdot 4$, but $5 \nmid 12$. Do not confuse $a \mid b$, which is a statement (true or false), with a/b , which is a number.

Divisibility facts are perfect practice for the direct proofs from the Proofs chapter.

Theorem 1. *If $a \mid b$ and $a \mid c$, then $a \mid (b + c)$.*

Proof. Since $a \mid b$ and $a \mid c$, there are integers j and k with $b = aj$ and $c = ak$. Then $b + c = aj + ak = a(j + k)$. Because $j + k$ is an integer, $a \mid (b + c)$. $\square$

7.1.1 The Division Algorithm

When b does not divide a evenly, there is a remainder. For any integer a and any positive integer b , there is exactly one way to write

$$a = qb + r \quad \text{with } 0 \leq r < b$$

The number q is the *quotient* and r is the *remainder*. In Python, $a // b$ gives q and $a \% b$ gives r . For example, $100 = 14 \cdot 7 + 2$, and $100 // 7$ is 14 while $100 \% 7$ is 2.

The remainder is never negative, even when a is: $-17 = (-4) \cdot 5 + 3$, so the remainder is 3, not -2 . Python agrees: $-17 \% 5$ is 3.

Exercise 38 **Quotients and Remainders**

Write each in the form $a = qb + r$ with $0 \leq r < b$.

Working Space

1. $a = 100, b = 7$
2. $a = 2026, b = 12$
3. $a = -17, b = 5$

Answer on Page 99

Exercise 39 **A Divisibility Proof**

Prove that if $a \mid b$ and $b \mid c$, then $a \mid c$.

Working Space

Answer on Page 99

7.2 Prime Numbers

A *prime* is an integer greater than 1 whose only positive divisors are 1 and itself. The first few are

$$2, 3, 5, 7, 11, 13, 17, 19, 23, 29, \dots$$

An integer greater than 1 that is not prime is *composite*. The number 1 is neither prime nor composite. (Leaving it out makes the next theorem work.)

Theorem 2 (Fundamental Theorem of Arithmetic). *Every integer greater than 1 can be written as a product of primes in exactly one way, apart from the order of the factors.*

For example, $360 = 2^3 \cdot 3^2 \cdot 5$. You can find a factorization by splitting off one factor at a time ($360 = 2 \cdot 180 = 2 \cdot 2 \cdot 90 = \dots$), and no matter which factors you split off first, you end up with the same primes. Primes are the atoms of multiplication: every whole number is built from them in exactly one way.

7.2.1 There Are Infinitely Many Primes

Primes get rarer as numbers get bigger. Do they ever run out? Euclid answered this around 300 BCE with one of the most famous proofs by contradiction ever written.

Theorem 3. *There are infinitely many primes.*

Proof. Suppose, for contradiction, that there are only finitely many primes, $p_1, p_2, \dots, p_k$. Let

$$N = p_1 p_2 \cdots p_k + 1$$

N is greater than 1, so it has at least one prime factor p . That prime must be one of $p_1, \dots, p_k$, so p divides the product $p_1 p_2 \cdots p_k$. Since p also divides N , it divides the difference $N - p_1 p_2 \cdots p_k = 1$. But no prime divides 1. This contradiction shows that our list could not have contained every prime. $\square$

7.2.2 Testing Whether a Number Is Prime

To check whether n is prime, you could try dividing it by every number from 2 to $n - 1$. You can stop much sooner. If $n = ab$ with $1 < a \leq b$, then $a \cdot a \leq a \cdot b = n$, so $a \leq \sqrt{n}$. In other words, a composite number always has a factor no bigger than its square root. So you only need to try primes up to $\sqrt{n}$. This is called *trial division*.

Example: Is 221 prime?

Solution: $\sqrt{221} \approx 14.9$, so we try the primes 2, 3, 5, 7, 11, and 13. The first five leave remainders, but $221 = 13 \cdot 17$. It is composite.

7.2.3 The Sieve of Eratosthenes

To find *all* the primes up to some limit, the Greek astronomer Eratosthenes had a cleverer idea. Write down the numbers from 2 to the limit. Circle 2 and cross out every multiple of 2. The next number not crossed out, 3, is prime: circle it and cross out its multiples. Repeat. Every number still standing at the end is prime. You can stop once you reach the square root of the limit, for the same reason as in trial division.

```

1 def primes_up_to(n):
2     is_prime = [True] * (n + 1)
3     is_prime[0] = is_prime[1] = False
4     for p in range(2, int(n ** 0.5) + 1):
5         if is_prime[p]:
6             # cross out every multiple of p, starting at p * p
7             for multiple in range(p * p, n + 1, p):

```

```

8         is_prime[multiple] = False
9     return [k for k in range(n + 1) if is_prime[k]]
10
11 print(primes_up_to(50))
12 print(len(primes_up_to(1_000_000)))

```

```

[2, 3, 5, 7, 11, 13, 17, 19, 23, 29, 31, 37, 41, 43, 47]
78498

```

There are 78,498 primes below one million, and the sieve finds them all in about a second.

Exercise 40 Factor and Test

Working Space

1. Find the prime factorization of 1001.
2. Is 391 prime? Which primes do you need to try?

Answer on Page 99

7.3 The Greatest Common Divisor

The *greatest common divisor* of two integers, $\gcd(a, b)$, is the largest integer that divides both. For example, $\gcd(12, 18) = 6$. If $\gcd(a, b) = 1$, we say a and b are *relatively prime*: they share no prime factor.

You could find a gcd by factoring both numbers, but factoring big numbers is hard. (That is the whole point of RSA!) Fortunately, there is a much faster way.

7.3.1 The Euclidean Algorithm

The key fact is this: if $a = qb + r$, then

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

Why? Any number that divides a and b also divides $r = a - qb$, and any number that divides b and r also divides $a = qb + r$. So the two pairs have exactly the same common divisors, and therefore the same greatest one.

So replace (a, b) by (b, r) and repeat. The numbers shrink every step, and when the remainder reaches 0, the last nonzero remainder is the gcd.

Example: Find $\text{gcd}(1071, 462)$.

Solution:

$$1071 = 2 \cdot 462 + 147$$

$$462 = 3 \cdot 147 + 21$$

$$147 = 7 \cdot 21 + 0$$

The last nonzero remainder is 21, so $\text{gcd}(1071, 462) = 21$. Three divisions, no factoring.

In Python, the algorithm is four lines long:

```

1 def gcd(a, b):
2     while b != 0:
3         a, b = b, a % b
4     return a
5
6 print(gcd(1071, 462))
7 print(gcd(252, 198))

```

21
18

(Python's `math` library also has a built-in `math.gcd`.) The Euclidean algorithm is fast even for numbers with hundreds of digits, because the remainders shrink by at least half every two steps.

7.3.2 The Extended Euclidean Algorithm

Running the algorithm backward reveals something surprising: the gcd can always be written as a combination of the two numbers. For any integers a and b , there are integers x and y with

$$ax + by = \text{gcd}(a, b)$$

This is called *Bézout's identity*. To find x and y , solve each step of the algorithm for its remainder, then substitute upward. For 1071 and 462:

$$\begin{aligned} 21 &= 462 - 3 \cdot 147 \\ &= 462 - 3 \cdot (1071 - 2 \cdot 462) \\ &= 7 \cdot 462 - 3 \cdot 1071 \end{aligned}$$

So $x = -3$ and $y = 7$: indeed, $1071(-3) + 462(7) = -3213 + 3234 = 21$. This back-substitution is exactly what RSA needs to build its secret key.

Exercise 41 Euclid by Hand

Working Space

1. Use the Euclidean algorithm to find $\gcd(252, 198)$.
2. Find integers x and y with $252x + 198y = \gcd(252, 198)$.

Answer on Page 100

7.4 Modular Arithmetic

If it is 9 o'clock now, what time will it be in 5 hours? Not 14 o'clock: the clock wraps around, and it will be 2 o'clock. You already do *modular arithmetic*: arithmetic where numbers wrap around after reaching a fixed value, called the *modulus*.

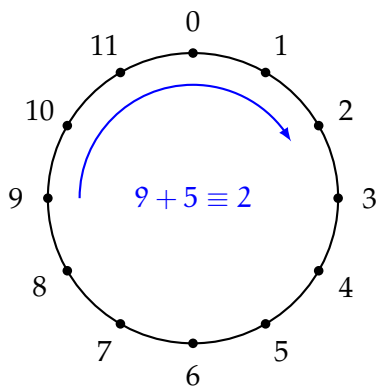


Figure 7.1: Arithmetic mod 12. Starting at 9 and moving 5 steps lands on 2.

Definition 1. Let n be a positive integer. We say a is congruent to b modulo n , written

$$a \equiv b \pmod{n}$$

if $n \mid (a - b)$. Equivalently, a and b leave the same remainder when divided by n .

For example, $14 \equiv 2 \pmod{12}$, $17 \equiv 2 \pmod{5}$, and $-1 \equiv 11 \pmod{12}$ (one hour before midnight is 11 o'clock).

The great thing about congruences is that you can reduce at any time. If $a \equiv b$ and $c \equiv d \pmod{n}$, then

$$a + c \equiv b + d \pmod{n} \quad \text{and} \quad ac \equiv bd \pmod{n}$$

So you can replace any number by its remainder before adding or multiplying. That keeps the numbers small, even when the true answer is enormous.

Example: What is the last digit of 3^{2026} ?

Solution: The last digit of a number is its remainder mod 10. The powers of 3 mod 10 are

$$3^1 \equiv 3, \quad 3^2 \equiv 9, \quad 3^3 \equiv 27 \equiv 7, \quad 3^4 \equiv 21 \equiv 1$$

Once we hit 1, the pattern repeats every 4 steps. Since $2026 = 4 \cdot 506 + 2$,

$$3^{2026} = (3^4)^{506} \cdot 3^2 \equiv 1^{506} \cdot 9 = 9 \pmod{10}$$

The last digit is 9, even though 3^{2026} has 967 digits.

7.4.1 Modular Inverses

In ordinary arithmetic, dividing by 3 means multiplying by $\frac{1}{3}$, the number whose product with 3 is 1. Mod n , there are no fractions, but there can still be a number that acts like $\frac{1}{3}$. An *inverse* of a modulo n is a number x with

$$ax \equiv 1 \pmod{n}$$

For example, $3 \cdot 4 = 12 \equiv 1 \pmod{11}$, so 4 is the inverse of 3 mod 11.

Not every number has an inverse. Mod 12, no multiple of 4 is ever 1 more than a multiple of 12. (Multiples of 4 are always multiples of 4, and $12k + 1$ never is.) In general, a has an inverse mod n exactly when $\gcd(a, n) = 1$, and the extended Euclidean algorithm finds it: if $ax + ny = 1$, then $ax \equiv 1 \pmod{n}$. In Python, `pow(a, -1, n)` computes it for you.

7.4.2 Fast Powers

RSA needs numbers like $m^e \bmod n$, where all three numbers have hundreds of digits. Multiplying m by itself e times would take longer than the age of the universe. Instead, use *repeated squaring*: square, reduce, square, reduce. To compute $5^{13} \bmod 23$, write $13 = 8 + 4 + 1$ and find

$$\begin{aligned} 5^1 &\equiv 5 \\ 5^2 &\equiv 25 \equiv 2 \\ 5^4 &\equiv 2^2 = 4 \\ 5^8 &\equiv 4^2 = 16 \end{aligned}$$

Then $5^{13} = 5^8 \cdot 5^4 \cdot 5^1 \equiv 16 \cdot 4 \cdot 5 = 320 \equiv 21 \pmod{23}$. That is five multiplications instead of twelve. For an exponent with 600 digits, it is a few thousand multiplications instead of a number with 600 digits. Python's three-argument `pow(m, e, n)` uses this method.

Exercise 42 Wrapping Around

Working Space

1. What is the last digit of 7^{2026} ?
2. Find the inverse of 5 modulo 12.
Check your answer.
3. Explain why 6 has no inverse modulo 9.

Answer on Page 100

7.5 Fermat's Little Theorem

Try raising numbers to the 6th power mod 7:

$$1^6 \equiv 1, \quad 2^6 = 64 \equiv 1, \quad 3^6 = 729 \equiv 1, \quad \dots, \quad 6^6 = 46656 \equiv 1 \pmod{7}$$

Every one is 1. That is no accident.

Theorem 4 (Fermat's Little Theorem). *If p is prime and $p \nmid a$, then*

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

Proof. Look at the $p - 1$ numbers $a, 2a, 3a, \dots, (p - 1)a$, reduced mod p . None of them is 0, because p divides neither a nor any of $1, \dots, p - 1$ (and a prime that divides a product must divide one of its factors). No two are equal either: if $ia \equiv ja$, then $p \mid (i - j)a$, so $p \mid (i - j)$, which is impossible for two different numbers between 1 and $p - 1$. So these are $p - 1$ different nonzero remainders, which means they are $1, 2, \dots, p - 1$ in some order. (For $p = 7$ and $a = 3$, they are 3, 6, 2, 5, 1, 4.)

Multiply all of them together. The two lists have the same product mod p :

$$a \cdot 2a \cdot 3a \cdots (p - 1)a \equiv 1 \cdot 2 \cdot 3 \cdots (p - 1) \pmod{p}$$

$$a^{p-1} \cdot (p - 1)! \equiv (p - 1)! \pmod{p}$$

Since p does not divide $(p - 1)!$, it has an inverse mod p . Multiplying both sides by that inverse leaves $a^{p-1} \equiv 1 \pmod{p}$. $\square$

Fermat's Little Theorem makes huge powers easy. To find $2^{100} \bmod 13$, note that $2^{12} \equiv 1$ and $100 = 8 \cdot 12 + 4$, so

$$2^{100} = (2^{12})^8 \cdot 2^4 \equiv 1^8 \cdot 16 \equiv 3 \pmod{13}$$

7.5.1 A Fast Primality Test

The theorem also gives a quick way to catch composite numbers. If $a^{n-1} \not\equiv 1 \pmod{n}$, then n is definitely not prime. Computers use this, with fast powers, to test numbers with hundreds of digits in a fraction of a second, far faster than trial division.

Passing the test does not prove n is prime, though. For example, $2^{340} \equiv 1 \pmod{341}$, but $341 = 11 \cdot 31$. A composite number that passes is called a *pseudoprime*. Trying a different base usually exposes it: $3^{340} \equiv 56 \pmod{341}$. Real primality tests use refined versions of this idea that no composite can fool.

Exercise 43 Using Fermat

Working Space

1. Use Fermat's Little Theorem to find $3^{100} \bmod 7$.
2. The number $561 = 3 \cdot 11 \cdot 17$ satisfies $2^{560} \equiv 1 \pmod{561}$. What does this

tell you about the Fermat test?

Answer on Page 100

7.6 RSA

Old ciphers had a weakness: the key that locks a message also unlocks it, so two people had to meet in secret to share a key first. In 1977, Ron Rivest, Adi Shamir, and Leonard Adleman published a way around this. In *public-key cryptography*, you have two keys. Your *public key* is like an open padlock: you hand out copies to everyone, and anyone can snap one shut on a box. Your *private key* opens the lock, and only you have it.

In RSA, a message is a number m . Encrypting and decrypting are two functions, and, just like the inverse functions you met in the Inverses and Transformations chapter, decrypting undoes encrypting.

7.6.1 Making the Keys

1. Choose two different large primes, p and q . Keep them secret.
2. Compute $n = pq$. This is public.
3. Compute $\varphi = (p - 1)(q - 1)$. Keep it secret.
4. Choose e with $\gcd(e, \varphi) = 1$. This is public. (65537 is a common choice.)
5. Compute d , the inverse of e modulo φ , with the extended Euclidean algorithm. This is your private key.

The public key is the pair (n, e) . To **encrypt** a message m (a number less than n), anyone computes

$$c = m^e \bmod n$$

To **decrypt**, you compute

$$m = c^d \bmod n$$

Example: Choose $p = 61$ and $q = 53$. Then $n = 3233$ and $\varphi = 60 \cdot 52 = 3120$. Take $e = 17$, which shares no factor with 3120. The extended Euclidean algorithm gives $d = 2753$; check: $17 \cdot 2753 = 46801 = 15 \cdot 3120 + 1$. To send $m = 65$, compute $c = 65^{17} \bmod 3233 = 2790$. Only someone who knows d can turn 2790 back into the message: $2790^{2753} \bmod 3233 = 65$.

Here is the whole thing in Python:

```

1  from math import gcd
2
3  # Key generation
4  p, q = 61, 53
5  n = p * q                # public
6  phi = (p - 1) * (q - 1)  # secret
7  e = 17                   # public
8  assert gcd(e, phi) == 1
9  d = pow(e, -1, phi)       # secret: the inverse of e mod phi
10 print("n =", n, " phi =", phi, " d =", d)
11
12 # Encrypt and decrypt a message
13 m = 65
14 c = pow(m, e, n)          # anyone can do this with (n, e)
15 print("ciphertext:", c)
16 print("decrypted:", pow(c, d, n)) # only the key owner knows d

```

```

n = 3233  phi = 3120  d = 2753
ciphertext: 2790
decrypted: 65

```

7.6.2 Why Decryption Works

Because $ed \equiv 1 \pmod{\varphi}$, we can write $ed = 1 + k(p-1)(q-1)$ for some integer k . Decrypting gives

$$c^d \equiv (m^e)^d = m^{ed} = m \cdot \left(m^{p-1}\right)^{k(q-1)} \pmod{p}$$

If $p \nmid m$, Fermat's Little Theorem says $m^{p-1} \equiv 1 \pmod{p}$, so $m^{ed} \equiv m \cdot 1 = m \pmod{p}$. If $p \mid m$, both sides are $0 \pmod{p}$, so again $m^{ed} \equiv m$. The same argument works $\pmod{q}$. So both p and q divide $m^{ed} - m$, and since they are different primes, so does their product n . Therefore $c^d \equiv m \pmod{n}$: decryption returns the original message.

7.6.3 Why It Is Secure

Everyone knows n and e . To find d , an attacker needs φ , and to find φ , they need p and q . That means factoring n . For our toy key, $n = 3233$ falls to trial division in an instant. Real RSA uses an n with 617 digits (2048 bits). The best known methods would need far longer than the age of the universe to factor it, while the key owner made n by multiplying, which takes a millisecond. RSA's security rests on that gap between multiplying and factoring.

Two notes from the real world. First, RSA as described here, called *textbook RSA*, is not safe to use as is; real systems add random padding to each message before encrypting. Second, a large enough quantum computer could factor n quickly, so cryptographers are already rolling out new “post-quantum” systems based on different hard problems.

Exercise 44 RSA by Hand

Alice picks $p = 5$ and $q = 11$, with public exponent $e = 3$.

Working Space

1. Find n , ϕ , and the private key d .
2. Bob encrypts the message $m = 9$. What ciphertext does he send?
3. Check that decrypting gives back 9. (A calculator or Python’s `pow` will help.)

Answer on Page 100

Exercise 45 Why Coprime?

In RSA, why must e satisfy $\gcd(e, \phi) = 1$? What goes wrong if, for example, $p = 5$, $q = 11$, and $e = 2$?

Working Space

Answer on Page 101

Exercise 46 Breaking a Small Key

You intercept a message encrypted with the public key $n = 391$, $e = 3$. Factor n , find d , and explain why this would be

Working Space

hopeless for a real key.

Answer on Page 101

Answers to Exercises

Answer to Exercise 1 (on page 8)

1. 2π
2. 60°
3. $\frac{5\pi}{4}$
4. 135°
5. $\frac{\pi}{6}$
6. $\frac{\pi}{4}$

Answer to Exercise 2 (on page 11)

$$180^\circ - (92^\circ + 42^\circ) = 46^\circ$$

Answer to Exercise 3 (on page 12)

$$360^\circ$$

Answer to Exercise 4 (on page 13)

(7, 7, 10): two sides match, so this is isosceles. (9, 40, 41): $9 + 40 = 49 > 41$ and no two sides match, so this is scalene. (3, 4, 9): $3 + 4 = 7$, which is less than 9, so this is not a triangle.

Answer to Exercise 5 (on page 14)

a: 10 because $6^2 + 8^2 = 10^2$

b: 12 because $5^2 + 12^2 = 13^2$

c: 8 because $8^2 + 15^2 = 17^2$

d: $3\sqrt{2} \approx 4.24$ because $3^2 + 3^2 = (3\sqrt{2})^2$

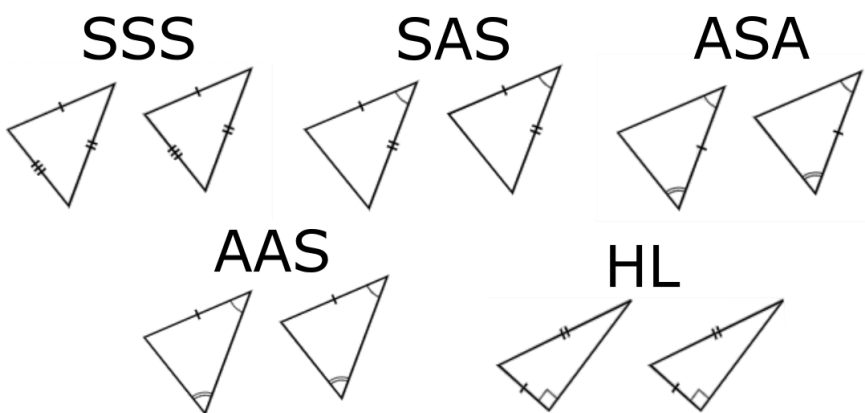
Answer to Exercise 6 (on page 22)

Congruent by the Side-Side-Right Congruency Test.

Congruent by the Side-Side-Side Congruency Test.

Congruent by the Side-Angle-Angle Congruency Test.

We do not know if they are congruent. The measured angle is not between the measured sides.



Answer to Exercise 7 (on page 23)

No. Every side of the second triangle is twice the matching side of the first, so the triangles are similar but not congruent.

Answer to Exercise 8 (on page 25)

The table has a radius of 3 meters.

So the area of its top is $3^2\pi \approx 28.27$ square meters.

$$28.27 \text{ square meters} \left(\frac{1 \text{ liter}}{6 \text{ square meters}} \right) \approx 4.71 \text{ liters}$$

Answer to Exercise 9 (on page 26)

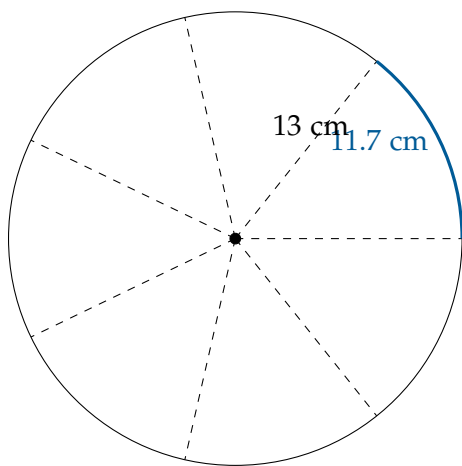
The diameter is

$$\frac{c}{\pi} = \frac{64}{\pi} \approx 20.37 \text{ centimeters}$$

Answer to Exercise 10 (on page 27)

The circumference of the pie is $26\pi \approx 81.7$ centimeters.

The length of the crust for each piece would be about $\frac{81.7}{7} = 11.7$ cm.



Answer to Exercise 11 (on page 29)

Rolling forward 10 cm unrolls 10 cm of tread, so the arc length is 10 cm. We need $r\theta = 10$ cm with $r = 25$ cm: $\theta = \frac{10 \text{ cm}}{25 \text{ cm}} = 0.4$ radians.

Answer to Exercise 12 (on page 29)

$$1. \frac{\pi}{4} \cdot 2 \text{ cm} = \frac{\pi}{2} \text{ cm}$$

2. $\pi \cdot 1 \text{ cm} = \pi \text{ cm}$

3. $\frac{\pi}{10} \cdot 5 \text{ cm} = \frac{\pi}{2} \text{ cm}$

4. $\frac{3\pi}{4} \cdot 3 \text{ cm} = \frac{9\pi}{4} \text{ cm}$

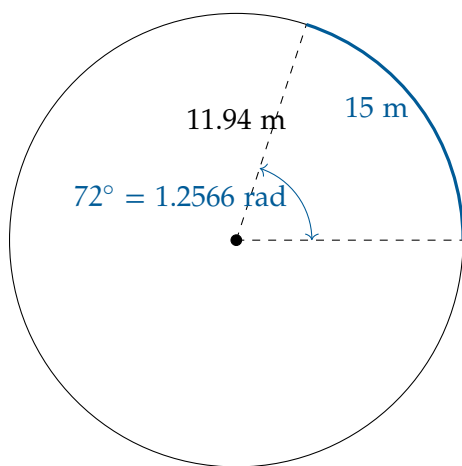
From longest to shortest: 4, 2, then 1 and 3 (which tie at $\frac{\pi}{2} \text{ cm}$).

Answer to Exercise 13 (on page 30)

$$72 \text{ degrees} \left(\frac{2\pi \text{ radians}}{360 \text{ degrees}} \right) \approx 1.2566 \text{ radians}$$

$$15 = 1.2566r$$

$$r = 11.94 \text{ meters}$$

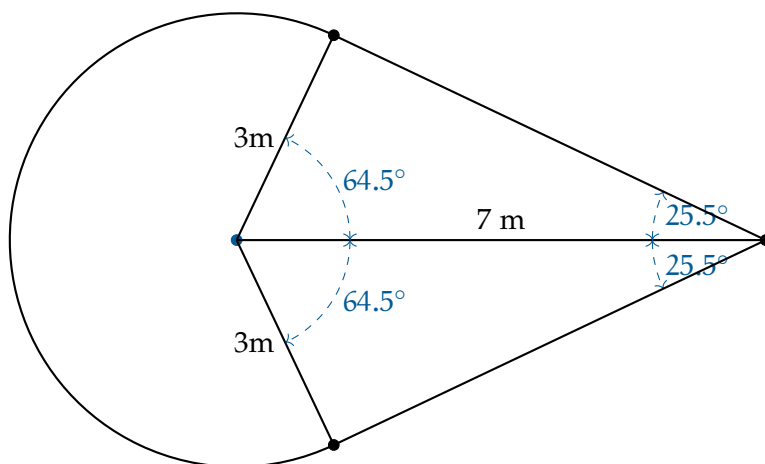


Answer to Exercise 14 (on page 31)

If the logo is 5 meters wide, the diameter is 5 meters and the radius is 2.5 meters. Using the formula for the area of a sector: $A_{\text{sector}} = \frac{1}{2} \frac{3\pi}{4} (2.5 \text{ m})^2 \approx 7.363 \text{ m}^2$. Since a liter covers 6 m^2 , you will need $\frac{7.363}{6} \approx 1.227 \text{ L}$ of paint.

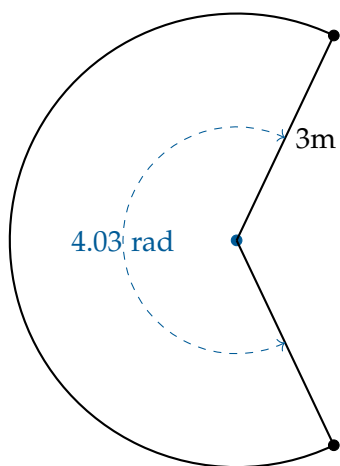
Answer to Exercise 15 (on page 34)

The trick: each tangent is perpendicular to its radius, so we get two right triangles:



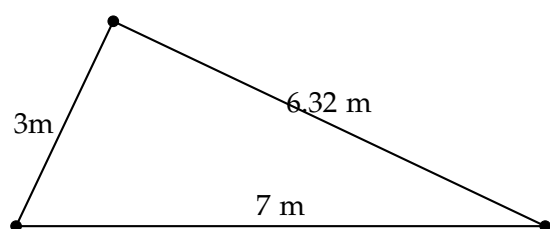
The sector has radius 3 and represents $360 - 2(64.5) = 231^\circ \approx 4.03$ radians.

The shape is this sector plus the two triangles. The sector is:



Its area is $\frac{1}{2}(4.03)(3^2) \approx 18.1$ square meters.

If a right triangle has a hypotenuse of 7m and one leg is 3m, the other leg is $\sqrt{7^2 - 3^2} = 2\sqrt{10} \approx 6.32$ m.



A right triangle with legs of 3 m and 6.32 m has an area of $\frac{1}{2}(3)(6.32) \approx 9.49$ square meters.

There are two of them, so the total area is $18.1 + 2(9.49) \approx 37.1$ square meters.

At six square meters per liter, you need $\frac{37.1}{6} \approx 6.2$ liters of paint.

Answer to Exercise 16 (on page 35)

You can only take the square root of nonnegative numbers, so the function is only defined when $x - 3 \geq 0$. Thus, the domain is all real numbers greater than or equal to 3.

Answer to Exercise 17 (on page 37)

The graph of this function is a line, its slope is -3 , and it intersects the y axis at $(0, 3)$.

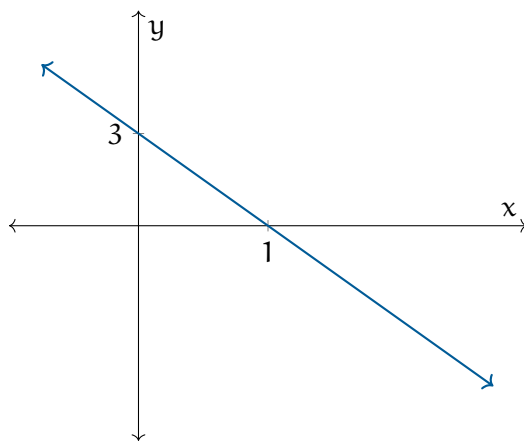


Figure 4.3: The graph of $f(x) = -3x + 3$.

Answer to Exercise 18 (on page 40)

It prints $-6 \ 0 \ 0$. The first value says the graph crosses the y -axis at $(0, -6)$. The two zeros

say $x = 3$ and $x = -2$ are the x -intercepts, the points where the parabola crosses the x -axis. Both match the Desmos graph.

Answer to Exercise 19 (on page 40)

This array skips 0. The two entries closest to it are $x \approx -0.0606$ and $x \approx 0.0606$, with $y \approx -16.5$ and $y \approx 16.5$. Matplotlib connects neighbors, so it draws a nearly vertical segment from $(-0.0606, -16.5)$ up to $(0.0606, 16.5)$. That segment belongs to neither branch of the graph. Plotting each side of the asymptote separately removes it. (With 101 points instead of 100, the array contains 0 exactly; NumPy then warns divide by zero and stores inf for that entry.)

Answer to Exercise 20 (on page 43)

It prints `2 0 0`. An even function needs $h(-1) = h(1)$, but $0 \neq 2$. Oddness requires $-h(-1) = h(1)$, which fails for the same reason. A single input that breaks a definition is enough to rule it out.

Answer to Exercise 21 (on page 43)

For `np.abs(x)`, the dashed $h(-x)$ curve lies exactly on the solid curve, and the tests print **True** then **False**: $|x|$ is even. With `x**3`, the dotted $-h(-x)$ curve lies on the solid curve, and the tests print **False** then **True**: x^3 is odd.

Answer to Exercise 22 (on page 45)

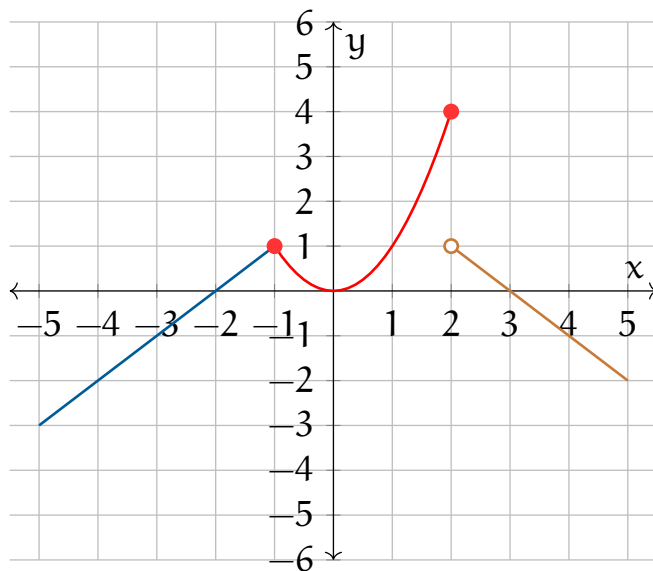
For $x \geq 0$, $|x| = x$. For $x < 0$, $|x| = -x$, which flips the negative number to a positive one. So,

$$|x| = \begin{cases} x & x \geq 0 \\ -x & x < 0 \end{cases}$$

Answer to Exercise 23 (on page 45)

First, let us create a table of values for each integer from -5 to 5:

x	-5	-4	-3	-2	-1	0	1	2	3	4	5
f(x)	-3	-2	-1	0	1	0	1	4	0	-1	-2



Answer to Exercise 24 (on page 47)

1.

$$C(x) = \begin{cases} 400x & 0 < x \leq 5 \\ 2000 + 350(x - 5) & 5 < x \leq 15 \\ 5500 + 300(x - 15) & x > 15 \end{cases}$$

2. $C(12) = 2000 + 350(12 - 5) = \$4450$

3. We need $\frac{C(x)}{x} < 360$. In the second case, $\frac{C(x)}{x} = 350 + \frac{250}{x}$, which stays above 360 for every $x \leq 15$. So we need the third case:

$$C(x) = 5500 + 300(x - 15) = 5500 + 300x - 4500 = 1000 + 300x$$

Now,

$$\frac{1000 + 300x}{x} < 360$$

$$\begin{aligned}
300 + \frac{1000}{x} &< 360 \\
\frac{1000}{x} &< 60 \\
1000 &< 60x \\
x &> \frac{1000}{60} \approx 16.67 \rightarrow 17
\end{aligned}$$

The hotel must buy at least 17 TVs. Check: $C(17) = \$6100$, and $\frac{6100}{17} \approx \$358.82$.

Answer to Exercise 25 (on page 50)

The outputs for $x = -5, -4, \dots, 5$ are $-3, -2, -1, 0, 1, 0, 1, 4, 0, -1, -2$, matching the table. At $x = -1$ the first condition fails ($-1 < -1$ is false), so Python uses x^2 and returns 1. At $x = 2$ the second condition includes 2, so Python returns $2^2 = 4$. Both are the closed circles on the graph.

Answer to Exercise 26 (on page 50)

The input 4 satisfies $x \geq 0$, so Python returns $4^2 = 16$ and never reaches the **elif**. Python does not flag overlapping cases; it takes the first match. Putting the special case first fixes it:

```

1 def q(x):
2     if x == 4:
3         return 10.2
4     elif x >= 0:
5         return x**2

```

Now $q(4)$ returns 10.2 and $q(3)$ returns 9. Ordering the checks this way does the same job as the condition $x \geq 0, x \neq 4$ in the revised definition.

Answer to Exercise 27 (on page 50)

It prints $-3 \ -2 \ 9 \ 7$. Flooring -2.5 moves down to -3 , the greatest integer less than or equal to -2.5 ; rounding toward zero would give -2 , which is wrong here. Its ceiling is -2 . An input of 8.00001 rises to 9, and an integer such as 7 comes back unchanged.

Answer to Exercise 28 (on page 51)

$g(-1) = 2(-1) + 5 = 3$. Solving $2x + 5 = 11$ gives $x = 3$.

Answer to Exercise 29 (on page 55)

This graph is the graph of $y = x^2$ that has been moved to the right by three units and up two units:

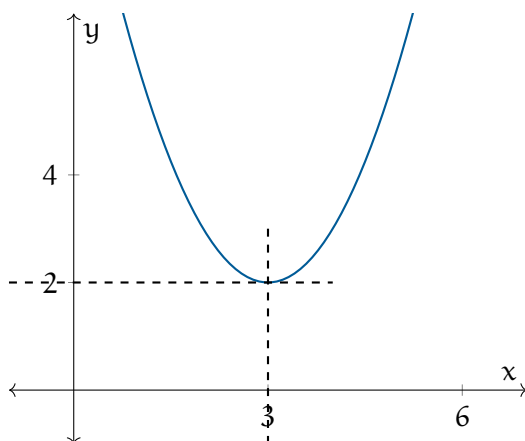


Figure 5.4: The graph of $f(x) = (x - 3)^2 + 2$.

To prevent any horizontal line from containing more than one point of the graph, you would need to use the left or the right side — either $\{x \in \mathbb{R} | x \leq 3\}$ or $\{x \in \mathbb{R} | x \geq 3\}$. Most people will choose the right side; the rest of the solution will assume that you did too.

To find the inverse we swap x and y : $x = (y - 3)^2 + 2$

Next, we solve for y to get the inverse: $y = \sqrt{x - 2} + 3$

You can take the square root of nonnegative numbers. So the function $f^{-1}(x) = \sqrt{x - 2} + 3$ is defined whenever x is greater than or equal to 2.

Answer to Exercise 30 (on page 55)

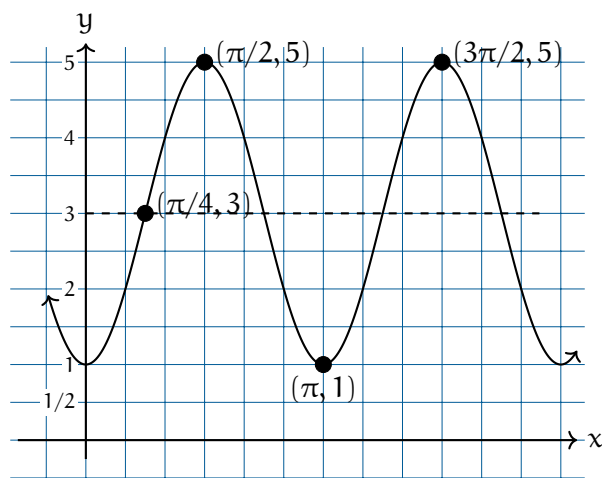
1. Not one-to-one. The quickest reason: $f(2) = f(6) = 2.0$. Also, from $x = 3$ to $x = 4$ the function rises from 3.6 to 5.3, so it passes through 4.0; from $x = 4$ to $x = 5$ it falls to 2.8, so it passes through 4.0 again.

2. Not one-to-one, even though no value in the table repeats. The function rises to 3.5 at $x = 4$, then falls to 3.1 at $x = 5$. Any value between 3.1 and 3.5, such as 3.2, is reached once on the way up and again on the way down.
3. Not one-to-one: the curve is symmetric about the y-axis, so a horizontal line through it hits twice.
4. One-to-one: the curve only goes down, so it passes the horizontal line test.
5. $f(t)$ would not be one-to-one because the football must pass through each height (except the peak height) both on the way up and on the way back down.
6. $v(t)$ is one-to-one because a falling object only speeds up, so each speed happens at exactly one time.

Answer to Exercise 31 (on page 57)

NumPy refuses to raise a negative decimal number to a fractional power, so every negative entry of $x^{1/3}$ becomes nan (“not a number”). For example, it returns nan for $(-8)^{1/3}$ even though the real cube root is -2 . Matplotlib skips nan points, which erases the left half. The function `np.cbrt` accepts negative inputs and returns -2 for -8 . The TikZ version of Figure 5.1 solves the same problem by graphing the left half as $-(-x)^{1/3}$.

Answer to Exercise 32 (on page 63)



This wave has an amplitude of 2; its baseline has been translated up to 3.

This wave has wavelength of π . A sine wave usually has a wavelength of 2π , so we need to compress the x axis by a factor of 2.

The crest is at $\frac{\pi}{2}$, so the wave crosses its baseline on the way up a quarter wavelength earlier, at $\frac{\pi}{2} - \frac{\pi}{4} = \frac{\pi}{4}$. A plain sine wave crosses its baseline on the way up at 0, so we translate right by $\frac{\pi}{4}$: replace x with $x - \frac{\pi}{4}$.

$$f(x) = 2 \sin \left(2 \left(x - \frac{\pi}{4} \right) \right) + 3 = 2 \sin \left(2x - \frac{\pi}{2} \right) + 3$$

Check: $f\left(\frac{\pi}{2}\right) = 2 \sin\left(\frac{\pi}{2}\right) + 3 = 5$ and $f(\pi) = 2 \sin\left(\frac{3\pi}{2}\right) + 3 = 1$. Watch the parentheses: $2 \sin(2x - \frac{\pi}{4}) + 3$ shifts right by only $\frac{\pi}{8}$.

Answer to Exercise 33 (on page 64)

Solve $x^3 = 8$. Then $x = 2$, so $f^{-1}(8) = 2$.

Answer to Exercise 34 (on page 68)

For what t is $-4.9t^2 + 12t + 2 = 0$? Start by dividing both sides of the equation by -4.9 .

$$t^2 - 2.45t - 0.408 = 0$$

The roots of this are at

$$x = -\frac{b}{2} \pm \frac{\sqrt{b^2 - 4c}}{2} = -\frac{-2.45}{2} \pm \frac{\sqrt{(-2.45)^2 - 4(-0.408)}}{2} = 1.225 \pm 1.382$$

The other root, $1.225 - 1.382 \approx -0.16$, is a time before you threw the hammer, so we ignore it.

$1.225 + 1.382 \approx 2.61$ seconds after releasing the hammer, it will hit the ground.

Answer to Exercise 35 (on page 71)

Factor as $(x - 2)(x + 2) = 0$. The solutions are $x = 2$ and $x = -2$.

Answer to Exercise 36 (on page 71)

1. Factor: $(x + 1)(x + 5) = 0$, so $x = -1$ or $x = -5$.
2. AC method: $ac = 6 = 6 \times 1$ and $6 + 1 = 7$, so $2x^2 + 6x + x + 3 = 2x(x + 3) + (x + 3) = (2x + 1)(x + 3) = 0$. So $x = -\frac{1}{2}$ or $x = -3$.
3. Complete the square: $x^2 - 10x + 25 = 7$, so $(x - 5)^2 = 7$ and $x = 5 \pm \sqrt{7}$, about 7.65 or 2.35.
4. The discriminant is $2^2 - 4(5) = -16 < 0$, so there are no real solutions.

Answer to Exercise 37 (on page 71)

Solve $-4.9t^2 + 8t + 2 = 3.05$, or $-4.9t^2 + 8t - 1.05 = 0$. With $a = -4.9$, $b = 8$, $c = -1.05$:

$$t = \frac{-8 \pm \sqrt{64 - 4(-4.9)(-1.05)}}{2(-4.9)} = \frac{-8 \pm \sqrt{43.42}}{-9.8} = \frac{8 \mp 6.59}{9.8}$$

So $t \approx 0.14$ s or $t \approx 1.49$ s. At 0.14 s, the ball is still rising past rim height. A ball cannot drop through the hoop from below, so the time that matters is 1.49 s, on the way down.

Answer to Exercise 38 (on page 74)

1. $100 = 14 \cdot 7 + 2$
2. $2026 = 168 \cdot 12 + 10$
3. $-17 = (-4) \cdot 5 + 3$

Answer to Exercise 39 (on page 74)

Since $a \mid b$, there is an integer j with $b = aj$. Since $b \mid c$, there is an integer k with $c = bk$. Substituting, $c = (aj)k = a(jk)$. Because jk is an integer, $a \mid c$.

Answer to Exercise 40 (on page 76)

1. $1001 = 7 \cdot 11 \cdot 13$.
2. $\sqrt{391} \approx 19.8$, so try 2, 3, 5, 7, 11, 13, 17, and 19. It is not divisible by 2 through 13, but $391 = 17 \cdot 23$. It is composite.

Answer to Exercise 41 (on page 78)

1.

$$252 = 1 \cdot 198 + 54$$

$$198 = 3 \cdot 54 + 36$$

$$54 = 1 \cdot 36 + 18$$

$$36 = 2 \cdot 18 + 0$$

So $\gcd(252, 198) = 18$.

2. Work backward:

$$\begin{aligned} 18 &= 54 - 36 = 54 - (198 - 3 \cdot 54) = 4 \cdot 54 - 198 \\ &= 4(252 - 198) - 198 = 4 \cdot 252 - 5 \cdot 198 \end{aligned}$$

So $x = 4$ and $y = -5$. Check: $1008 - 990 = 18$.

Answer to Exercise 42 (on page 80)

1. The powers of 7 mod 10 are 7, 9, 3, 1, then repeat every 4. Since $2026 = 4 \cdot 506 + 2$, $7^{2026} \equiv 7^2 \equiv 9$. The last digit is 9.
2. $5 \cdot 5 = 25 = 2 \cdot 12 + 1 \equiv 1 \pmod{12}$, so 5 is its own inverse.
3. $\gcd(6, 9) = 3$, not 1. Every multiple of 6 is a multiple of 3, and so is every number of the form $9k$, so $6x - 9k$ is always a multiple of 3 and can never equal 1.

Answer to Exercise 43 (on page 81)

1. $3^6 \equiv 1 \pmod{7}$ and $100 = 16 \cdot 6 + 4$, so $3^{100} \equiv 3^4 = 81 \equiv 4 \pmod{7}$.
2. 561 is composite but passes the test for base 2, so passing the Fermat test does not prove a number is prime. (561 is a *Carmichael number*: it passes for every base that shares no factor with it.)

Answer to Exercise 44 (on page 84)

1. $n = 55$ and $\varphi = 4 \cdot 10 = 40$. We need $3d \equiv 1 \pmod{40}$; since $3 \cdot 27 = 81 = 2 \cdot 40 + 1$, $d = 27$.
2. $c = 9^3 \bmod 55 = 729 \bmod 55 = 14$.
3. $14^{27} \bmod 55 = 9$, the original message. In Python, `pow(14, 27, 55)` returns 9.

Answer to Exercise 45 (on page 84)

The private key d is the inverse of e modulo φ , and an inverse exists only when $\gcd(e, \varphi) = 1$. With $\varphi = 40$ and $e = 2$, $\gcd(2, 40) = 2$, so no d exists. In fact, encryption is not even one-to-one: $2^2 = 4$ and $53^2 = 2809 = 51 \cdot 55 + 4$, so the messages 2 and 53 both encrypt to 4, and nobody could tell which one was sent.

Answer to Exercise 46 (on page 84)

$391 = 17 \cdot 23$ (from the Factor and Test exercise). Then $\varphi = 16 \cdot 22 = 352$. Since $3 \cdot 235 = 705 = 2 \cdot 352 + 1$, $d = 235$. A real key has a 617-digit n , and no known method can factor a number that size in any reasonable amount of time.



INDEX

- AC method, 70
- acute angle, 6
- acute triangle, 11
- amplitude, 60
- angle, 5
- arc length, 28
- array, 39
- arrays, 39
- asymptote, 37
- asymptotes, 37

- Bézout's identity, 78
- Bézout's identity, 77

- ceiling function, 46
- center, 25
- chord, 33
- circle
 - area of, 25
- circumference, 26
- complementary angles, 6
- completing the square, 65, 66
- composite, 74
- congruent, 19, 79
- CPCTC, 22

- degrees, 7
- Desmos, 38
- diameter, 26
- difference of squares, 70
- discriminant, 66

- distance
 - in 3 dimensions, 17
- distance formula, 17
- distance using Pythagorean theorem, 15
- divides, 73
- divisibility, 73
- division algorithm, 73
- divisor, 73
- domain, 35
- dot product, 18

- equilateral triangle, 8
- Euclidean algorithm, 76
- even function, 41, 64

- factor, 73
- factoring, 69
- Fermat primality test, 81
- Fermat's Little Theorem, 80
- floor function, 46
- function, 35
- function transformations, 58
- Fundamental Theorem of Arithmetic, 74

- greatest common divisor, 76

- horizontal line test, 54
- hypotenuse, 10, 14

- interior angles, 10
- inverse, 53, 79
- inverse function, 53

- isosceles triangle, 9
- legs of a right triangle, 14
- line segment, 5
- lines, 5
- magnitude, 17
- modular arithmetic, 78
- modular exponentiation, 80
- modular inverse, 79
- modulus, 78
- multiple, 73
- number theory, 73
- obtuse angle, 6
- obtuse triangle, 11
- odd function, 41, 64
- one-to-one, 54
- one-to-one function, 54
- order of transformations, 62
- parallel, 17
- perpendicular, 18
- piecewise functions, 44
- prime, 74
- prime number, 74
- private key, 82
- pseudoprime, 81
- public key, 82
- public-key cryptography, 82
- Pythagorean theorem, 14
- Pythagorean triples, 14
- quadratic equation, 65
- quadratic formula, 68
- quadratic function, 65
- quadrilateral, 12
- quotient, 73
- radians, 7
- radius, 25
- range, 35, 54
- ray, 5
- reflections, 20, 53
- relation, 35
- relatively prime, 76
- remainder, 73
- repeated squaring, 80
- right angle, 6
- right triangle, 10
- rigid transformation, 19
- roots, 66, 98
- rotations, 20
- RSA, 73, 82
- Scalene Triangle, 9
- secant, 33
- sector, 31
- side-angle-angle, 20
- side-angle-side, 21
- side-side-angle, 22
- side-side-side, 20
- Sieve of Eratosthenes, 75
- similar triangles, 20
- special right triangles, 14
- sphere, 26
- supplementary angles, 6
- symmetry, 64
- tangent, 32
- tangent line, 32
- transformations, 19
- translation
 - horizontal, 59
 - vertical, 59
- translations, 20
- transversal, 7
- trial division, 75
- triangle, 8
- triangle inequality, 10
- vector, 17
- vertex formula, 66
- vertical line test, 38
- wavelength, 61
- zero product property, 69