MATH 34001

Fundamental Concepts of Algebra*

Instructor: Darci L. Kracht

Kent State University

April 22, 2015

0 Introduction

We will begin our study of mathematics this semester with the familiar notion of even and odd integers. We define them formally and then prove some of their properties.

Definition 1. An integer n is ***even*** if $n = 2k$ for some integer k.

Question 2. Is 0 even? Why or why not?

Definition 3. An integer n is ***odd*** if $n = 2k + 1$ for some integer k.

Divisibility by 2: Many of us are familiar with the statements below. Formulate precise statements of each and then prove them formally.

Proposition 4. Even plus even is even.

Proposition 5. Even plus odd is odd.

Proposition 6. Odd plus odd is even.

Proposition 7. Even times even is even.

Proposition 8. Even times odd is even.

Proposition 9. Odd times odd is odd.

Exercise 10. Grade the work of student Sam Pull below. It may be correct, completely incorrect, or somewhere in between.

Proposition. If x and y are even integers, then $x + y$ is an even integer.

Sam Pull's Proof. Suppose x and y are even but $x + y$ is odd. Then for some integer k, $x + y = 2k + 1$. Therefore, $x + y + (-2)k = 1$. The left side of the equation is even because it is the sum of even numbers. However, the right side of the equation is odd. Since an even cannot equal an odd, we have a contradiction. Therefore, $x + y$ is even. ■

---

*Based on notes by Donald L. White (Kent State University) and Matthew G. Jones (California State University Dominguez Hills). Used with permission.

1 Number Systems

Notation 11. The following notation will be used throughout the course.

$\mathbb{N} = \{1, 2, 3, \ldots\}$ is the set of ***natural numbers***.

$\mathbb{W} = \{0, 1, 2, 3, \ldots\}$ is the set of ***whole numbers***.

$\mathbb{Z} = \{0, \pm 1, \pm 2, \pm 3, \ldots\}$ is the set of ***integers***. ("Z" is for "Zahlen," German for "numbers.")

$\mathbb{Q} = \left\{ \frac{a}{b} \middle| a, b \in \mathbb{Z}, b \neq 0 \right\}$ is the set of ***rational numbers***. ("Q" is for "quotient.")

$\mathbb{R}$ is the set of ***real numbers***.

$\mathbb{C}$ is the set of ***complex numbers***.

The sets $\mathbb{Q}$, $\mathbb{R}$, and $\mathbb{C}$ will be defined later in the course. We record the notation here for completeness.

1.1 Binary operations

Definition 12. A ***binary operation*** is an operation on a set that combines two elements in the set to produce another element in the set.

Definition 13. A set is said to be ***closed*** under a binary operation if the combination of *any* two elements in the set is itself an element of that set.

Exercise 14. Determine whether the set $\mathbb{N}$ is closed under each of the familiar binary operations $+, -, \times, \div$. (Here, and always, you will be expected to *explain* your answer.)

Exercise 15. Determine whether the set $\mathbb{W}$ is closed under each of the familiar binary operations $+, -, \times, \div$.

Exercise 16. Determine whether the set $\mathbb{Z}$ is closed under each of the familiar binary operations $+, -, \times, \div$.

1.2 The integers

The familiar binary operations addition and multiplication are considered basic operations on $\mathbb{N}$ and $\mathbb{Z}$ and we will not define them here. Subtraction and division are defined in terms of addition and multiplication, respectively, as we shall soon see. First, let us review some algebraic properties of addition and multiplication.

Definition 17. Algebraic Properties Let S be a set on which binary operations $\star$ and $\circ$ are defined. We define the following (potential) properties.

a. **Associative Law of $\star$:** $a \star (b \star c) = (a \star b) \star c$ for all $a, b, c \in S$.

b. **Commutative Law of $\star$:** $a \star b = b \star a$ for all $a, b \in S$.

c. **Left Distributive Law of $\circ$ over $\star$:** $c \circ (a \star b) = c \circ a \star c \circ b$ for all $a, b, c \in S$.

d. **Right Distributive Law of $\circ$ over $\star$:** $(a \star b) \circ c = a \circ c \star b \circ c$ for all $a, b, c \in S$.

Exercise 18. What properties of addition or multiplication of $\mathbb{N}$ are illustrated by each of the following? State the name of the property and write it out carefully.

a. $5 + (7 + 9) = 5 + (9 + 7)$

b. $6 + (2 + 3) = (2 + 3) + 6$

c. $5 + (7 + 9) = (5 + 7) + 9$

d. Compute $3 + 4 + 8$

e. $2 \cdot (3 \cdot 5) = 2 \cdot (5 \cdot 3)$

f. Compute $3 \cdot 4 \cdot 5$

g. $2 \cdot (3 \cdot 5) = (3 \cdot 2) \cdot 5$

h. $3 \cdot (5 + 7) = 3 \cdot 5 + 3 \cdot 7$

Definition 19. The number 0 is said to be an ***additive identity element*** since, for any number a, $a + 0 = a$.

Definition 20. For a number a, the negative of a, written $-a$, is called an ***additive inverse*** of a since $a + (-a) = 0$.

Fact 21. a. If a number system has an additive identity, it is unique.

b. If an element a in a number system has an additive inverse, it is unique.

Exercise 22. Determine whether each of the sets $\mathbb{N}$ and $\mathbb{Z}$ is closed under the taking of additive inverses.

Definition 23. The binary operation ***subtraction*** is defined by

$$a - b = a + (-b),$$

for numbers a, b.

Question 24. Do the algebraic properties of $\mathbb{N}$ discussed in Exercise 18 hold for addition and multiplication in $\mathbb{Z}$ as well? Do they hold for subtraction in $\mathbb{Z}$?

Problem 25. Propose definitions for ***multiplicative identity element*** and ***multiplicative inverse***.

Fact 26. a. If a number system has an multiplicative identity, it is unique.

b. If an element a in a number system has an multiplicative inverse, it is unique.

Proposition 27. If $n \in \mathbb{Z}$, then $0 \cdot n = 0$. *[Hint: Start with the fact that $0 + 0 = 0$ (why?) and use the distributive law.]*

Proposition 28. If $a \in \mathbb{Z}$, then $-(-a) = a$.

Proposition 29. If $a \in \mathbb{Z}$, then $(-1) \cdot a = -a$.

Corollary 30. It is true that $(-1) \cdot (-1) = 1$.

Proposition 31. If $a, b \in \mathbb{Z}$, then $(-a) \cdot (-b) = a \cdot b$.

Notation 32. The multiplicative inverse of an element a is denoted by $\frac{1}{a}$ or by a^{-1}.

Exercise 33. Determine whether each of the sets $\mathbb{N}$ and $\mathbb{Z}$ is closed under the taking of multiplicative inverses.

Definition 34. The binary operation ***division*** is defined by

$$a \div b = \frac{a}{b} = a \times \frac{1}{b},$$

for all numbers a, b for which this makes sense.

Question 35. Why is division by 0 undefined?

1.3 Rational numbers

Definition 36. The ***set*** $\mathbb{Q}$ ***of rational numbers*** is defined to be the set of all quotients of integers, i.e.,

$$\mathbb{Q} = \left\{ \frac{a}{b} \middle| a, b \in \mathbb{Z}, b \neq 0 \right\}$$

We define ***equivalence***, ***addition***, and ***multiplication*** in $\mathbb{Q}$ as follows. For $a, b, c, d, a', b' \in \mathbb{Z}$,

i. $\frac{a}{b} = \frac{a'}{b'}$ if and only if $ab' = ba'$.

ii. $\frac{a}{b} + \frac{c}{d} = \frac{ad + bc}{bd}$.

iii. $\frac{a}{b} \cdot \frac{c}{d} = \frac{ac}{bd}$.

Proposition 37. Every integer is a rational number. *That is,* $\mathbb{Z} \subseteq \mathbb{Q}$.

Proposition 38. If $q = \frac{a}{b} \in \mathbb{Q}$ with $q \neq 0$, then $q^{-1} = \frac{b}{a}$.

That is, the multiplicative inverse of $\frac{a}{b}$ *is* $\frac{b}{a}$.

Proposition 39. Multiplication in $\mathbb{Q}$ is well-defined.

That is, if $\frac{a}{b} = \frac{\hat{a}}{\hat{b}}$ *and* $\frac{c}{d} = \frac{\hat{c}}{\hat{d}}$, *where* $a, b, \hat{a}, \hat{b}, c, d, \hat{c}, \hat{d} \in \mathbb{Z}$, *then* $\frac{a}{b} \cdot \frac{c}{d} = \frac{\hat{a}}{\hat{b}} \cdot \frac{\hat{c}}{\hat{d}}$.

For each of the following, first restate the result precisely, in symbols.

Proposition 40. Multiplication in $\mathbb{Q}$ is commutative.

Proposition 41. Multiplication in $\mathbb{Q}$ is associative.

Proposition 42. Addition in $\mathbb{Q}$ is well-defined.

Proposition 43. Addition in $\mathbb{Q}$ is commutative.

Proposition 44. Addition in $\mathbb{Q}$ is associative.

1.4 Real numbers

Recall that the usual way we write numbers is using a base-ten positional system. Each digit is one of $0, 1, 2, \ldots, 9$ and the value is determined by its position. For example,

$$5672 = 5 \cdot 10^3 + 6 \cdot 10^2 + 7 \cdot 10^1 + 2 \cdot 10^0,$$

and

$$0.381 = 3 \cdot 10^{-1} + 8 \cdot 10^{-2} + 1 \cdot 10^{-3}.$$

Definition 45. The ***decimal representation*** or ***decimal expansion*** of a positive number r is a representation of the form

$$\begin{aligned} r &= n_k n_{k-1} \ldots n_2 n_1 n_0 \,.\, d_1 d_2 d_3 \ldots \\ &= n_k \cdot 10^k + n_{k-1} \cdot 10^{k-1} + \cdots + n_2 \cdot 10^2 + n_1 \cdot 10^1 + n_0 \cdot 10^0 + d_1 \cdot 10^{-1} + d_2 \cdot 10^{-2} + d_3 \cdot 10^{-3} + \cdots, \end{aligned}$$

where $n_0, n_1, \ldots n_k, d_1, d_2, d_3, \ldots \in \{0, 1, 2, \ldots, 9\}$.

Definition 46. The decimal representation of a number is said to be ***repeating*** if it becomes ***periodic*** (repeating its values at regular intervals) and the infinitely-repeated portion is not zero. The infinitely-repeated digit sequence is called the ***repetend***. The length of the shortest repetend is called the ***period*** of the repeating decimal number. If the repetend is zero, the decimal representation is called a ***terminating*** decimal.

Exercise 47. Perform the long division by hand to find the decimal expansion, terminating or repeating, of each of the following rational numbers.

a. $\dfrac{3}{20}$ b. $\dfrac{1}{3}$ c. $\dfrac{1}{9}$ d. $\dfrac{1}{7}$

e. $\dfrac{3}{7}$ f. $\dfrac{5}{6}$ g. $\dfrac{1}{11}$ h. $\dfrac{1}{17}$

Question 48. What is the maximum period of a rational number a/b with repeating decimal expansion? Why?

Proposition 49. Every rational number has either a terminating or a repeating decimal expansion.

Exercise 50. Convert the following repeating decimal numbers to fractions in lowest terms.

a. $0.393939\ldots = 0.\overline{39}$

b. $4.302302302\ldots = 4.\overline{302}$

c. $57.13478478478\ldots = 57.13\overline{478}$

d. $106.106537253725372\ldots = 106.106\overline{5372}$

Exercise 51. Let's think about the decimal number $0.\overline{9} = 0.999\ldots$ in a few different ways.

a. Multiply your decimal expansion for $\dfrac{1}{3}$ (from Exercise 47) by 3. What do you get? Now multiply the fraction $\dfrac{1}{3}$ by 3.

b. Use your decimal expansion for $\frac{1}{9}$ (from Exercise 47) to find decimal expansions for $\frac{2}{9}$, $\frac{3}{9}$, $\frac{4}{9}$, and so on. What is the decimal expansion for $\frac{9}{9} = 9 \cdot \frac{1}{9}$? But what is $\frac{9}{9}$?

c. Use the method of Exercise 50 to convert $0.\overline{9} = 0.999\ldots$ to a fraction in lowest terms.

d. Can you explain what's going on here?

Proposition 52. Every terminating or repeating decimal number is the decimal expansion of a rational number.

Definition 53. We define the set of ***real numbers***, $\mathbb{R}$, to be the set of all decimal expansions. The real numbers that have neither terminating nor repeating decimal expansions are called ***irrational numbers***.

Fact 54. The following properties hold in $\mathbb{R}$.

i. $\mathbb{R}$ is closed under addition;

ii. Addition in $\mathbb{R}$ is associative;

iii. Addition in $\mathbb{R}$ is commutative;

iv. The additive identity element of $\mathbb{R}$ is 0;

v. The additive inverse of a in $\mathbb{R}$ is $-a$;

vi. $\mathbb{R}$ is closed under multiplication;

vii. Multiplication in $\mathbb{R}$ is associative;

viii. Multiplication in $\mathbb{R}$ is commutative;

ix. The multiplicative identity element of $\mathbb{R}$ is 1;

x. If $a \neq 0$, the multiplicative inverse of a in $\mathbb{R}$ is $1/a$;

xi. Multiplication distributes over addition in $\mathbb{R}$.

This says that $\mathbb{R}$ is an example of an algebraic structure called a ***field***.

Proposition 55. Any irrational number can be approximated to any desired degree of accuracy by a rational number.

Proposition 56. The square-root of 2, $\sqrt{2}$, is irrational.

The following two propositions can be proven using a similar technique, using definitions and results from later in the course.

Proposition 57. The square-root of 3, $\sqrt{3}$, is irrational.

Proposition 58. If p is a prime number, then $\sqrt{p}$, is irrational.

1.5 Complex numbers

1.5.1 The algebra of complex numbers

Definition 59. We define the set of ***complex numbers***, $\mathbb{C}$, to be the set of all numbers of the form $a + bi$, where $a, b \in \mathbb{R}$ and i is the ***imaginary unit***, satisfying $i^2 = -1$. We define ***equivalence***, ***addition***, and ***multiplication of complex numbers*** as follows. For $a + bi, c + di \in \mathbb{C}$, where $a, b, c, d \in \mathbb{R}$,

i. $a + bi = c + di$ if and only if $a = c$ and $b = d$;

ii. $(a + bi) + (c + di) = (a + c) + (b + d)i$;

iii. $(a + bi) \cdot (c + di) = (ac - bd) + (ad + bc)i$.

Proposition 60. Every real number is a complex number. That is, $\mathbb{R} \subseteq \mathbb{C}$.

Exercise 61. Compute each of the following, expressing your answer in ***standard form***, $a + bi$, where $a, b \in \mathbb{R}$.

a. $(2 + 5i) + (-3 + 7i)$

b. $(2 + 5i) \cdot (-3 + 7i)$

c. $i(10 - 8i)$

d. $(9 - 2i) \cdot (9 + 2i)$

Definition 62. Let $z = a + bi \in \mathbb{C}$ where $a, b \in \mathbb{R}$. Then

i. the ***real part*** of z is $\mathrm{Re}(z) = a$,

ii. the ***imaginary part*** of z is $\mathrm{Im}(z) = b$.

Exercise 63. Find each of the following.

a. $\mathrm{Re}(5 - 7i)$

b. $\mathrm{Im}(5 - 7i)$

c. $\mathrm{Re}(188)$

d. $\mathrm{Im}(188)$

e. $\mathrm{Re}(\sqrt{37}i)$

f. $\mathrm{Im}(\sqrt{37}i)$

g. $\mathrm{Re}(1 + \sqrt{2} - 3i)$

h. $\mathrm{Im}(1 + \sqrt{2} - 3i)$

Note 64. Definition 59(i) can be restated as follows: Two complex numbers z, w are equal if and only if $\mathrm{Re}(z) = \mathrm{Re}(w)$ and $\mathrm{Im}(z) = \mathrm{Im}(w)$.

Exercise 65. Find all pairs of real numbers (x, y) satisfying each of the following.

a. $[x + yi] + [(2x - y) + (y - x)i] = 17 - 9i$

b. $(1 + yi)(x + 7i) = 19 - 3i$

c. $\left(\frac{1}{2} + \frac{1}{4}i\right)\left(\frac{1}{3} + yi\right) = x - \frac{1}{4}i$

d. $(x + yi)(y - xi) = 6 + 8i$

e. $(x + yi)(y + xi) = 4i$

f. $(x + yi)(y + xi) = 1 + 2i$

Proposition 66. The following properties hold in $\mathbb{C}$.

i. The set $\mathbb{C}$ is closed under addition.

ii. Addition in $\mathbb{C}$ is associative.

iii. Addition in $\mathbb{C}$ is commutative.

iv. The additive identity element of $\mathbb{C}$ is 0.

v. If $z = a + bi$, where $a, b \in \mathbb{R}$, then $-z$, the additive inverse of z in $\mathbb{C}$, is $(-a) + (-b)i$.

Definition 67. If $z = a + bi \in \mathbb{C}$, where $a, b \in \mathbb{R}$, the ***complex conjugate*** of z is $\bar{z} = a - bi$.

Exercise 68. Evaluate each of the following, writing your answer in ***standard form***, $a + bi$, where $a, b \in \mathbb{R}$.

a. $\overline{6 + 10i}$ b. $\overline{-2 - 5i}$ c. $\overline{\sqrt{2}i}$ d. $\overline{17}$

Proposition 69. i. If $r \in \mathbb{R}$, then $\bar{r} = r$.

ii. Let $z \in \mathbb{C}$. If $\bar{z} = z$, then $z \in \mathbb{R}$.

Exploration 70. Evaluate each of the following, being careful to follow the specified order of operations.

a. $\overline{(5 - 6i) + (2 + i)}$ c. $\overline{(-1 - 9i) + 8i}$ e. $\overline{(11 + 37i) + 13}$

b. $\overline{(5 - 6i)} + \overline{(2 + i)}$ d. $\overline{(-1 - 9i)} + \overline{8i}$ f. $\overline{(11 + 37i)} + \overline{13}$

State and prove a conjecture based on these examples.

Exploration 71. Evaluate each of the following, being careful to follow the specified order of operations.

a. $\overline{(2 - 3i) \cdot (5 + i)}$ c. $\overline{(5 + 7i) \cdot 10i}$ e. $\overline{(1 + i) \cdot (-4 - 6i)}$

b. $\overline{(2 - 3i)} \cdot \overline{(5 + i)}$ d. $\overline{(5 + 7i)} \cdot \overline{10i}$ f. $\overline{(1 + i)} \cdot \overline{(-4 - 6i)}$

State and prove a conjecture based on these examples.

Exploration 72. Evaluate each of the following. Then state and prove a conjecture based on these examples.

a. $\overline{\overline{(10 - 8i)}}$ b. $\overline{\overline{(-7 + 2i)}}$ c. $\overline{\overline{13i}}$ d. $\overline{\overline{51}}$

Exploration 73. Evaluate each of the following. Then state and prove a conjecture based on these examples.

a. $(10 - 8i) + \overline{(10 - 8i)}$ c. $(1 + i) + \overline{(1 + i)}$ e. $13i + \overline{13i}$

b. $(-7 + 2i) + \overline{(-7 + 2i)}$ d. $50 + \overline{50}$ f. $(\sqrt{2} + \sqrt{3}i) + \overline{(\sqrt{2} + \sqrt{3}i)}$

Exploration 74. Evaluate each of the following. Then state and prove a conjecture based on these examples.

a. $(10 - 8i) - \overline{(10 - 8i)}$ c. $(1 + i) - \overline{(1 + i)}$ e. $13i - \overline{13i}$

b. $(-7 + 2i) - \overline{(-7 + 2i)}$ d. $50 - \overline{50}$ f. $(\sqrt{2} + \sqrt{3}i) - \overline{(\sqrt{2} + \sqrt{3}i)}$

Exploration 75. Evaluate each of the following. Then state and prove a conjecture based on these examples.

a. $(10 - 8i) \cdot \overline{(10 - 8i)}$ c. $(1 + i) \cdot \overline{(1 + i)}$ e. $13i \cdot \overline{13i}$

b. $(-7 + 2i) \cdot \overline{(-7 + 2i)}$ d. $50 \cdot \overline{50}$ f. $(\sqrt{2} + \sqrt{3}i) \cdot \overline{(\sqrt{2} + \sqrt{3}i)}$

Exploration 76. Evaluate each of the following.

a. $(10-8i)\cdot\dfrac{\overline{(10-8i)}}{100+64}$

b. $(-7+2i)\cdot\dfrac{\overline{(-7+2i)}}{49+4}$

c. $13i\cdot\dfrac{\overline{13i}}{169}$

d. $(1+i)\cdot\dfrac{\overline{(1+i)}}{1+1}$

State and prove a conjecture about the existence and form of multiplicative inverses in $\mathbb{C}$ based on these examples.

Exercise 77. Evaluate each of the following, writing your answer in standard form. *Hint: The best approach to take is analogous to rationalizing the denominator of a radical expression.*

a. $\dfrac{5-4i}{-2+7i}$

b. $\dfrac{10}{9+4i}$

c. $\dfrac{1+i}{3i}$

Exploration 78. Write each of the following in standard form.

a. i^3

b. i^4

c. i^5

d. i^6

e. i^7

f. i^8

g. i^{100}

h. i^{1001}

i. i^{589}

j. i^{3762}

Find a general rule for simplifying i^n for positive integers n. Explain why it works.

1.5.2 The geometry of complex numbers

Definition 79. The ***Argand plane*** is the two dimensional rectangular coordinate system whose points are in one-to-one correspondence with the set of complex numbers as follows. We associate the complex number $z = a + bi$, where $a, b \in \mathbb{R}$, with the point (a, b) in the plane. The horizontal axis is called the ***real axis*** and the vertical axis is called the ***imaginary axis***.

Exploration 80. Plot each of the following in an Argand plane.

a. $1+3i$

b. $\overline{1+3i}$

c. $-2+5i$

d. $\overline{-2+5i}$

e. $-4i$

f. $\overline{-4i}$

g. 2.5

h. $\overline{2.5}$

How are z and $\overline{z}$ related geometrically?

Exploration 81. a. In an Argand plane:

(i) Plot the complex number $z = 2 + 10i$ and then sketch the segment from the origin O to z in black ink.

(ii) Plot the complex number $w = 8 + 4i$ and then sketch the segment from the origin O to w in blue ink.

(iii) Plot the complex number $z + w$ and then sketch the segment from the origin O to $z + w$ in red ink.

(iv) Sketch the segment from z to $z + w$ in blue ink.

(v) Sketch the segment from w to $z + w$ in black ink.

b. In another Argand plane:

(i) Plot the complex number $z = -6 + 2i$ and then sketch the segment from the origin O to z in black ink.

(ii) Plot the complex number $w = 3 + 5i$ and then sketch the segment from the origin O to w in blue ink.

(iii) Plot the complex number $z + w$ and then sketch the segment from the origin O to $z + w$ in red ink.

(iv) Sketch the segment from z to $z + w$ in blue ink.

(v) Sketch the segment from w to $z + w$ in black ink.

c. In another Argand plane:

(i) Plot the complex number $z = -5$ and then sketch the segment from the origin O to z in black ink.

(ii) Plot the complex number $w = 2i$ and then sketch the segment from the origin O to w in blue ink.

(iii) Plot the complex number $z + w$ and then sketch the segment from the origin O to $z + w$ in red ink.

(iv) Sketch the segment from z to $z + w$ in blue ink.

(v) Sketch the segment from w to $z + w$ in black ink.

d. Speculate on a geometric interpretation of addition of complex numbers. Play around with more examples if needed.

Exploration 82. How are z and $-z$ related geometrically? *(Plot a bunch of different examples, make a conjecture, and then explain why it's true.)*

Exploration 83. Plot each complex number z in an Argand plane, sketch the segment from the origin O to z, and then find the length of that segment.

a. $z = -1 + 2i$ b. $z = 4 - 5i$ c. $z = -6i$ d. $z = 3/2$

Derive a formula for the distance from the origin O to a general complex number $z = a + bi$, where $a, b \in \mathbb{R}$.

Definition 84. If $z = a + bi$ is a complex number, where $a, b \in \mathbb{R}$, define the ***modulus*** or ***magnitude*** of z, denoted $|z|$, by

$$|z| = \sqrt{a^2 + b^2}.$$

Question 85. What is a geometric interpretation of $|z|$?

Exercise 86. Describe the locus of points in the complex plane satisfying each of the following.

a. $|z| = 5$ b. $|z| = 0$ c. $|z| = -3$

Exercise 87. For $z \in \mathbb{C}$ with $z \neq 0$, give an expression for $\frac{1}{z}$, the multiplicative inverse of z, in terms of the modulus of z.

Proposition 88. If $z \in \mathbb{C}$, then $|z| = \sqrt{z\overline{z}}$.

Proposition 89. If $z \in \mathbb{C}$ and r is a nonnegative real number, then $|rz| = r|z|$

The following series of lemmas leads to an important result called the Triangle Inequality.

Lemma 90. If $z \in \mathbb{C}$, then $|z|^2 = \mathrm{Re}(z)^2 + \mathrm{Im}(z)^2$.

Lemma 91. If $z \in \mathbb{C}$, then $|z|^2 \geq \mathrm{Re}(z)^2$ and $|z|^2 \geq \mathrm{Im}(z)^2$.

Lemma 92. If $z \in \mathbb{C}$, then $|z| \geq \mathrm{Re}(z)$ and $|z| \geq \mathrm{Im}(z)$.

Lemma 93. If $z, w \in \mathbb{C}$, then $|z + w|^2 \leq |z|^2 + |w|^2$.

Theorem 94 (The Triangle Inequality)**.** If $z, w \in \mathbb{C}$, then $|z + w| \leq |z| + |w|$.

Question 95. Why is the previous theorem called the Triangle Inequality?

Definition 96. For a nonzero complex number z, the angle (in radians) between the positive real axis and the line segment from the origin O to z is called the ***argument*** of z and is denoted $\arg z$. The argument of 0 is undefined.

Question 97. For a nonzero complex number z, $\arg z$ is not unique. Why not?

Definition 98. For a nonzero complex number z, the (unique) value of $\arg z$ that lies in the interval $(-\pi, \pi]$ is called the ***principal value of the argument*** and is denoted $\mathrm{Arg}\, z$.

Exercise 99. For each complex number z, find $|z|$ and $\mathrm{Arg}\, z$. *(Hint: Think trigonometry!)*

a. $z = 5i$

b. $z = -i$

c. $z = 10$

d. $z = -1/5$

e. $z = 1 + i$

f. $z = \dfrac{\sqrt{3}}{2} + \dfrac{1}{2}i$

Proposition 100. Let $z = a + bi \in \mathbb{C}$, where $a, b \in \mathbb{R}$. If $r = |z|$ and $\theta = \arg z$, then

$$a = r\cos\theta \text{ and } b = r\sin\theta.$$

Corollary 101. Let $z = a + bi \in \mathbb{C}$, where $a, b \in \mathbb{R}$. If $r = |z|$ and $\theta = \arg z$, then

$$r = \sqrt{a^2 + b^2} \text{ and } \tan\theta = \frac{b}{a}.$$

Definition 102. If $z \in \mathbb{C}$, then the ***polar form*** of z is

$$z = r(\cos\theta + i\sin\theta),$$

where $r = |z|$ and $\theta = \arg z$. *(For the sake of consistency, we will usually use $\theta = \mathrm{Arg}\, z$.)*

Exercise 103. Find the standard form of each of the following complex numbers. Plot each in the complex plane. *Give exact values, without using a calculator.*

a. $\cos\dfrac{3\pi}{4} + i\sin\dfrac{3\pi}{4}$

b. $4\left[\cos\left(-\dfrac{\pi}{6}\right) + i\sin\left(-\dfrac{\pi}{6}\right)\right]$

c. $7\left(\cos\dfrac{22\pi}{3} + i\sin\dfrac{22\pi}{3}\right)$

d. $\dfrac{3}{8}\left(\cos 3\pi + i\sin 3\pi\right)$

e. $\sqrt{3}\left[\cos\left(-\dfrac{\pi}{2}\right) + i\sin\left(-\dfrac{\pi}{2}\right)\right]$

f. $\pi\left(\cos 8\pi + i\sin 8\pi\right)$

Exercise 104. Find the polar form of each of the following complex numbers, using the principal value of the argument. Plot each in the complex plane. *Give exact values, without using a calculator.*

a. $5i$

b. $-i$

c. 10

d. $-1/5$

e. $1+i$

f. $\dfrac{\sqrt{3}}{2}+\dfrac{1}{2}i$

g. $-5\sqrt{3}+5i$

h. $\dfrac{7}{\sqrt{2}}-\dfrac{7}{\sqrt{2}}i$

i. $-1-\sqrt{3}i$

Exploration 105. We will explore the relationship between the modulus of a product and the moduli of the factors.

a. For each pair of complex numbers, compute zw.

(i) $z=5i$, $w=1+i$

(ii) $z=-8$, $w=-\dfrac{\sqrt{3}}{2}-\dfrac{1}{2}i$

(iii) $z=5\sqrt{3}+5i$, $w=2+2\sqrt{3}i$

(iv) $z=\dfrac{7}{\sqrt{2}}+\dfrac{7}{\sqrt{2}}i$, $w=3\sqrt{2}-3\sqrt{2}i$

b. For each pair of complex numbers above, find $|z|$, $|w|$, and $|zw|$.

c. Conjecture a relationship between the modulus of a product and the moduli of the factors.

Exploration 106. We will explore the relationship between the argument of a product and the arguments of the factors.

a. For each pair of complex numbers, compute zw. *(You've already done this above.)*

(i) $z=5i$, $w=1+i$

(ii) $z=-8$, $w=-\dfrac{\sqrt{3}}{2}-\dfrac{1}{2}i$

(iii) $z=5\sqrt{3}+5i$, $w=2+2\sqrt{3}i$

(iv) $z=\dfrac{7}{\sqrt{2}}+\dfrac{7}{\sqrt{2}}i$, $w=3\sqrt{2}-3\sqrt{2}i$

b. For each pair of complex numbers above, find $\operatorname{Arg} z$, $\operatorname{Arg} w$, and $\operatorname{Arg}(zw)$.

c. Conjecture a relationship between the argument of a product and the argument of the factors.

Exploration 107. We will explore the relationship between the modulus of a complex number and the modulus of its multiplicative inverse.

a. Let $z=1-i$.

(i) Find $|z|$.

(ii) Find $\dfrac{1}{z}$.

(iii) Find $\left|\dfrac{1}{z}\right|$

b. Repeat with each of the following.

(i) $z=-7i$

(ii) $z=5\sqrt{3}+5i$

(iii) $z=3\sqrt{2}-3\sqrt{2}i$

c. Conjecture a relationship between the modulus of a complex number and the modulus of its multiplicative inverse.

Exploration 108. We will explore the relationship between the argument of a complex number and the argument of its multiplicative inverse.

a. For each z in the previous exploration,

(i) Find $\operatorname{Arg} z$.

(ii) Find $\operatorname{Arg} \frac{1}{z}$.

b. Conjecture a relationship between the argument of a complex number and the argument of its multiplicative inverse.

Theorem 109. For $r, s, \theta, \phi \in \mathbb{R}$,

$$[r(\cos\theta + i\sin\theta)] \cdot [s(\cos\phi + i\sin\phi)] = rs[\cos(\theta+\phi) + i\sin(\theta+\phi)].$$

Exercise 110. For each pair of complex numbers, convert to polar form, then compute zw.

a. $z = 5i$
$w = 1 + i$

b. $z = -8$
$w = -\frac{\sqrt{3}}{2} - \frac{1}{2}i$

c. $z = 5\sqrt{3} + 5i$
$w = 2 + 2\sqrt{3}i$

d. $z = \frac{7}{\sqrt{2}} + \frac{7}{\sqrt{2}}i$
$w = 3\sqrt{2} - 3\sqrt{2}i$

Theorem 111 (DeMoivre)**.** For $r, \theta \in \mathbb{R}$,

$$[r(\cos\theta + i\sin\theta)]^n = r^n(\cos n\theta + i\sin n\theta).$$

Corollary 112. For $r, \theta \in \mathbb{R}$, with $r \neq 0$,

$$\frac{1}{r(\cos\theta + i\sin\theta)} = \frac{1}{r}[\cos(-\theta) + i\sin(-\theta)].$$

Exercise 113. Use polar form to calculate each of the following. Write your answers in standard form.

a. $\left(-\frac{\sqrt{3}}{2} - \frac{1}{2}i\right)^{13}$

b. $(1-i)^5$

c. $\left(-\sqrt{2} + \sqrt{2}i\right)^{10}$

2 Basic Number Theory

2.1 Divisibility in the integers

We reviewed the familiar notions of even and odd in the Introduction to this course. Our goal now is to generalize this idea to account for divisibility by any nonzero integer d.

Definition 114. If $d, m \in \mathbb{Z}$ with $d \neq 0$, we write $d|m$ and say "d divides m" to mean that there is an integer k such that $dk = m$. If d does not divide m, then we write $d \nmid m$.

Caution!. "Divides" is a relation, not an operator. The symbol is a vertical bar (like half of an absolute value symbol), and *not* the solidus or slash that represents the operation of division. The *statement* $3|12$ is read "three divides twelve" and has a *truth* value (in this case, true). On the other hand, the *expression* $3/12$ is read "three divided by twelve" and has a *numerical* value (in this case, 0.25). When writing these symbols, make sure it is clear which one you intend.

Definition 115. Let $m \in \mathbb{Z}$. We say that m is ***even*** if $2|m$. We say that m is ***odd*** if $2 \nmid m$.

Exercise 116. Explain why Definition 115 is equivalent to Definitions 1 and 3.

Exercise 117. Restate Proposition 4 using the notation of Definition 115. *Do you remember how to prove it?*

Exercise 118. Restate Proposition 5 using the notation of Definition 115. *Do you remember how to prove it?*

Exercise 119. Restate Proposition 6 using the notation of Definition 115. *Do you remember how to prove it?*

Can we generalize these propositions to divisibility by other integers?

Exercise 120. First consider divisibility by 3. Prove or find a counter example to each of the following conjectures. Let $m, n \in \mathbb{Z}$ for each.

a. If $3|m$ and $3|n$, then $3|(m+n)$.

b. If $3|m$ but $3 \nmid n$, then $3 \nmid (m+n)$.

c. If $3 \nmid m$ and $3 \nmid n$, then $3|(m+n)$.

d. If $3 \nmid m$ and $3 \nmid n$, then $3 \nmid (m+n)$.

Exercise 121. Next consider divisibility by 6. Prove or find a counter example to each of the following conjectures. Let $m, n \in \mathbb{Z}$ for each.

a. If $6|m$ and $6|n$, then $6|(m+n)$.

b. If $6|m$ but $6 \nmid n$, then $6 \nmid (m+n)$.

c. If $6 \nmid m$ and $6 \nmid n$, then $6|(m+n)$.

d. If $6 \nmid m$ and $6 \nmid n$, then $6 \nmid (m+n)$.

Now consider the general cases. Prove or give a counter example to each of the following.

Conjecture 122. Let $d, m, n \in \mathbb{Z}$ with $d \neq 0$. If $d|m$ and $d|n$, then $d|(m+n)$.

Conjecture 123. Let $d, m, n \in \mathbb{Z}$ with $d \neq 0$. If $d|m$ but $d \nmid n$, then $d \nmid (m+n)$.

Conjecture 124. Let $d, m, n \in \mathbb{Z}$ with $d \neq 0$. If $d \nmid m$ and $d \nmid n$, then $d|(m+n)$.

Conjecture 125. Let $d, m, n \in \mathbb{Z}$ with $d \neq 0$. If $d \nmid m$ and $d \nmid n$, then $d \nmid (m+n)$.

Exercise 126. Restate Proposition 7 using the notation of Definition 115. *Do you remember how to prove it?*

Exercise 127. Restate Proposition 8 using the notation of Definition 115. *Do you remember how to prove it?*

Exercise 128. Restate Proposition 9 using the notation of Definition 115. *Do you remember how to prove it?*

Can we generalize these propositions to divisibility by other integers?

Exercise 129. First consider divisibility by 3. Prove or find a counter example to each of the following conjectures. Let $m, n \in \mathbb{Z}$ for each.

a. If $3|m$ and $3|n$, then $3|mn$.

b. If $3|m$ but $3 \nmid n$, then $3 \nmid mn$.

c. If $3 \nmid m$ and $3 \nmid n$, then $3|mn$.

d. If $3 \nmid m$ and $3 \nmid n$, then $3 \nmid mn$.

Exercise 130. Next consider divisibility by 6. Prove or find a counter example to each of the following conjectures. Let $m, n \in \mathbb{Z}$ for each.

a. If $6|m$ and $6|n$, then $6|mn$.

b. If $6|m$ but $6 \nmid n$, then $6 \nmid mn$.

c. If $6 \nmid m$ and $6 \nmid n$, then $6|mn$.

d. If $6 \nmid m$ and $6 \nmid n$, then $6 \nmid mn$.

Now consider the general cases. Prove or give a counter example to each of the following.

Conjecture 131. Let $d, m, n \in \mathbb{Z}$ with $d \neq 0$. If $d|m$ and $d|n$, then $d|mn$.

Conjecture 132. Let $d, m, n \in \mathbb{Z}$ with $d \neq 0$. If $d|m$ but $d \nmid n$, then $d \nmid mn$.

Conjecture 133. Let $d, m, n \in \mathbb{Z}$ with $d \neq 0$. If $d \nmid m$ and $d \nmid n$, then $d|mn$.

Conjecture 134. Let $d, m, n \in \mathbb{Z}$ with $d \neq 0$. If $d \nmid m$ and $d \nmid n$, then $d \nmid mn$.

Proposition 135. Let $d, m, n \in \mathbb{Z}$ with $d \neq 0$. If $d|m$ *or* $d|n$, then $d|mn$.

Exercise 136. Let $d, m, n \in \mathbb{Z}$ with $d \neq 0$. If $d \nmid m$ and $d \nmid n$, then d may or may not divide the sum $m + n$. Show two examples for which it works and two examples for which it fails.

Question 137. Let p be a prime and m, and n be integers. If $p \nmid m$ and $p \nmid n$, is it possible for p to divide the sum $m + n$? *(Support your answer with an explanation and evidence. However, you need not provide a formal proof, since we haven't defined "prime" yet.)*

Exercise 138. Grade the work of student Sam Pull below. It may be correct, completely incorrect, or somewhere in between.

Proposition. Let d be an integer and let m and n be integers. If $d|m$ and $d|n$, then $d|(m + n)$.

Sam Pull's Proof. Suppose $d|m$ and $d|n$. Then for some integer k, $dk = m$ and $dk = n$. Then $m + n = dk + dk = 2dk = d(2k)$, so $d|(m + n)$. ■

Proposition 139. Let a and d be integers. If $a > 0$ and $d|a$, then $d \leq a$.

Proposition 140. If a and b are integers with $a|b$ and $b|a$, then $a = \pm b$.

Definition 141. Suppose $d, m \in \mathbb{Z}$. If $m = dq + r$, for some $q, r \in \mathbb{Z}$ with $0 \leq r < d$, then q is called the ***quotient*** and r is called the ***remainder*** upon division of m by d.

It is helpful to note that in the notation of the definition, $m - r = dq$. This shows that the difference of m and the remainder r is a multiple of d.

Exercise 142. Give three examples of pairs of integers d and m. Exactly two of your pairs should have nonzero remainders. State the values of the quotient and remainder in all three examples.

It must be *proved* that the quotient and remainder in Definition 141 exist and are unique. The theorem that asserts this is called the Division Algorithm. This is within the scope of this course, but we will skip the proof this semester, due to lack of time. Although the Division Algorithm is familiar from elementary school, it is also important. There are many situations in algebra where we do not have the ability to find quotients and remainders.

Theorem 143 (The Division Algorithm: Existence)**.** Given a natural number d, for every $n \in \mathbb{N}$, there are integers q and r so that $r = n - dq$ with $0 \leq r < d$.

In mathematics, it is often useful to know that there is only one answer. In the case of the division algorithm, this allows us to speak of *the* quotient and *the* remainder, instead of *a* quotient and *a* remainder. This brings us to the following:

Theorem 144 (The Division Algorithm: Uniqueness)**.** Given a natural number d and a natural number n, if n can be written as $n = dq + r$, where $0 \leq r < d$, and also as $n = dq' + r'$, where $0 \leq r' < d$, and with $q, q', r, r' \in \mathbb{Z}$, then $q = q'$ and $r = r'$.

2.2 Modular arithmetic

Exercise 145. For each of the following, consider a typical 12-hour clock, ignoring designations of "am" or "pm."

a. If it is now 8 o'clock, what time will it be in 8 hours?

b. If a doctor works a 24-hour shift starting at 5 o'clock, what time will it be when her shift ends?

c. A lawyer with a big case coming up starts working at 12 o'clock and completes his billable hours for the case at 12 o'clock. What can you say about how long the lawyer worked?

d. A team of 5 people, working against a deadline, starts Monday at 6 o'clock. The team members work 8-hour shifts one after another. If every team member works one shift, what time will it be when they finish? (Ignore the day of the week.)

e. Three workers complete back-to-back shifts of equal length. If it was 7 o'clock when the first worker started his shift, and 4 o'clock when the third worker ended her shift, what can you say about the length of the shifts?

Exercise 146. Pop is sold in packs of 6 cans. In each of the following scenarios, determine how many leftover cans will not be able to be packaged into 6-packs.

a. 14 cans of pop

b. 37 cans of pop

c. You have one carton of 14 cans of pop and 37 cans on a shelf.

d. You have 14 shelves, each with 37 cans of pop.

e. 32 cans of pop

f. You have 3 shelves of 32 cans of pop.

Conjecture 147. In the context of Exercise 146, can you make general conjectures about how many cans of pop will be left over based on how many cans you start with? Try to formulate conjectures that would cover all possible cases. *Hint: Use the idea of remainders.*

Definition 148. Let $n \in \mathbb{N}$. For two integers a and b, we say that a ***is congruent to*** b ***modulo*** n and write

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

if $n|(a-b)$.

Exercise 149. What is the set of all integers a such that $a \equiv 1 \pmod{2}$? Explain.

Exercise 150. What is the set of all integers a such that $a \equiv 2 \pmod{10}$? Explain.

Exercise 151. What is the set of all integers a such that $a \equiv r \pmod{n}$? Explain.

Definition 152. The set referred to in Exercise 151 is called the ***equivalence class*** r ***modulo*** n or ***congruence class*** r ***modulo*** $n$and is denoted $\overline{r}$.

Definition 153. Fix a particular $n \in \mathbb{N}$. Notice that every integer belongs to exactly one congruence class mod n. We define $\mathbb{Z}_n$, the ***integers modulo*** n, to be the set of all congruence classes modulo n. These congruence classes can be written $\overline{0}, \overline{1}, \overline{2}, \ldots, \overline{n-2}, \overline{n-1}$. Because of what we discovered (and will prove later) about divisibility, we can define operations of addition and multiplication on $\mathbb{Z}_n$.

Exercise 154. Restate each of the clock scenarios in Exercise 145 as an equation in modular arithmetic.

Exercise 155. Restate each of the six-pack scenarios in Exercise 146 as an equation in modular arithmetic.

Exercise 156. Ordinary operations involve modulo 10. When adding, for instance $879 + 426$, the first thing many people do is "9 plus 6 equals 5, carry the 1." Rewrite this as a statement in modular arithmetic.

Example 157. Perpetual calendars, those that will tell you what day of the week it was on any date in the past or future , are built using modular arithmetic. In general, any kind of cyclic behavior can be thought of as involving modular arithmetic. Examples include 12-month calendars, the 12 signs of the Western or Chinese zodiac, and aerobics counting or musical counting (1-2-3, 1-2-3, 1-2-3,).

Proposition 158. If $a_0 \equiv a_1 \pmod{n}$ and $b_0 \equiv b_1 \pmod{n}$, then $a_0 + b_0 \equiv a_1 + b_1 \pmod{n}$. (This means that addition modulo n does not depend on which member of the congruence class is chosen, and so it is well-defined.)

Proposition 159. If $a_0 \equiv a_1 \pmod{n}$ and $b_0 \equiv b_1 \pmod{n}$, then $a_0 \cdot b_0 \equiv a_1 \cdot b_1 \pmod{n}$. (This means that multiplication modulo n does not depend on which member of the congruence class is chosen, and so it is well-defined.)

Definition 160. The integer r with $0 \leq r \leq n-1$ and $a \equiv r \pmod{n}$ is called the ***least (nonnegative) residue of*** a ***modulo*** n.

Note that the least nonnegative residue of a modulo n is simply the remainder on division of a by n.

Exercise 161. Make an addition table for $\mathbb{Z}_3$, the integers modulo 3.

Exercise 162. Make an addition table for $\mathbb{Z}_6$, the integers modulo 6.

Exercise 163. Make a multiplication table for $\mathbb{Z}_3$, the integers modulo 3.

Exercise 164. Make a multiplication table for $\mathbb{Z}_6$, the integers modulo 6.

Exercise 165. Use your multiplication table to complete the following.

a. Find all solutions $\overline{x}$ to the equation $\overline{3} \cdot \overline{x} = \overline{3}$ in $\mathbb{Z}_6$.

b. Find all integer solutions x to the congruence equation $3x \equiv 3 \pmod{6}$.

Exercise 166. Use your multiplication table to complete the following.

a. Find all solutions $\overline{x}$ to the equation $\overline{3} \cdot \overline{x} = \overline{1}$ in $\mathbb{Z}_6$.

b. Find all integer solutions x to the congruence equation $3x \equiv 1 \pmod{6}$.

Exercise 167. Use your multiplication table to complete the following.

a. Find all solutions $\overline{x}$ to the equation $\overline{5} \cdot \overline{x} = \overline{4}$ in $\mathbb{Z}_6$.

b. Find all integer solutions x to the congruence equation $5x \equiv 4 \pmod{6}$.

Exercise 168. Use your multiplication table to complete the following.

a. Find all solutions $\overline{x}$ to the equation $\overline{5} \cdot \overline{x} = \overline{1}$ in $\mathbb{Z}_6$.

b. Find all integer solutions x to the congruence equation $5x \equiv 1 \pmod{6}$.

Question 169. Based on your addition tables above, does $\mathbb{Z}_n$ have an additive identity element? If so, which congruence class is it? Why?

Question 170. Based on your multiplication tables above, does $\mathbb{Z}_n$ have a multiplicative identity element? If so, which congruence class is it? Why?

Proposition 171. If $n \in \mathbb{Z}$, then $n(n+1) \equiv 0 \pmod 2$.

Proposition 172. If $n \in \mathbb{Z}$ is odd, then $n^2 \equiv 1 \pmod 8$.

Proposition 173. If $a \in \mathbb{Z}$, then $a^2 \equiv 0$ or $1 \pmod 4$.

Notice from your work above that some elements in $\mathbb{Z}_6$ have multiplicative inverses and others do not. For this reason, we make the following definition.

Definition 174. The ***set of units of*** $\mathbb{Z}_n$ is defined to be

$$\mathbb{Z}_n^\times = \{\overline{k} \in \mathbb{Z}_n | \text{ there is some } \overline{r} \in \mathbb{Z}_n \text{ such that } \overline{k} \cdot \overline{r} = \overline{1}\}.$$

Exercise 175. Determine the congruence classes that are in $\mathbb{Z}_5^\times$.

Exercise 176. Determine the congruence classes that are in $\mathbb{Z}_6^\times$.

Exercise 177. Determine the congruence classes that are in $\mathbb{Z}_{15}^\times$.

Definition 178. A nonzero integer n is said to be ***composite*** if there exist integers a and b, with neither a nor b equal to ± 1, such that $n = ab$.

Proposition 179. If n is a composite number, then there are two numbers k and m so that $km \equiv 0 \pmod n$, but $k \not\equiv 0 \pmod n$ and $m \not\equiv 0 \pmod n$.

Definition 180. A nonzero integer p is said to be ***prime*** if $p \neq \pm 1$ and, for every pair of integers a and b, if $p|ab$, then $p|a$ or $p|b$.

Proposition 181. Suppose p is prime and $m, n \in \mathbb{Z}$. If $mn \equiv 0 \pmod p$, then either $m \equiv 0 \pmod p$ or $n \equiv 0 \pmod p$.

Theorem 182. If $m \in \mathbb{Z}$ with $m \neq \pm 1$, then there is a prime p such that $p|m$.

Theorem 183. If p is prime and $k \in \mathbb{Z}$ with $0 < k < p$, then $\overline{0}, \overline{k}, \overline{2k}, \overline{3k}, \ldots, \overline{(p-1)k}$ are all distinct members of $\mathbb{Z}_p$.

Theorem 184. If p is prime, then $\mathbb{Z}_p^\times$ includes all congruence classes of $\mathbb{Z}_p$ except for $\overline{0}$.

Definition 185. A ***common divisor*** of integers m and n is an integer d such that $d|m$ and $d|n$.

Definition 186. Let m and n be integers, at least one of which is not zero. The ***greatest common divisor*** of m and n is the largest integer d such that $d|m$ and $d|n$. We denote the greatest common divisor of m and n by $\gcd(m, n)$.

Exploration 187. a. Verify that $\gcd(6, 10) = 2$.

b. Find each of the following.

(i) $\gcd(12, 20) = \gcd(2 \cdot 6, 2 \cdot 10)$

(ii) $\gcd(30, 50) = \gcd(5 \cdot 6, 5 \cdot 10)$

(iii) $\gcd(42, 70) = \gcd(7 \cdot 6, 7 \cdot 10)$

(iv) $\gcd(60, 100) = \gcd(10 \cdot 6, 10 \cdot 10)$

c. Make a conjecture based on these calculations. (We do not have all of the tools needed to prove it.)

Exploration 188. a. Note again that $\gcd(6, 10) = 2$. Find $\gcd\left(\frac{6}{2}, \frac{10}{2}\right) = \gcd(3, 5)$.

b. Show that $\gcd(24, 54) = 6$. Find $\gcd\left(\frac{24}{6}, \frac{54}{6}\right) = \gcd(4, 9)$.

c. Make a conjecture based on these calculations. (We do not have all of the tools needed to prove it.)

Definition 189. Two integers m and n are said to ***relatively prime*** (or ***coprime***) if $\gcd(m, n) = 1$.

We don't have the tools to prove the following two theorems, but they might be useful later in the course.

Theorem 190. Let $k, m, n \in \mathbb{Z}$. If $m|k$ and $n|k$ and $\gcd(m, n) = 1$, then $(mn)|k$.

Theorem 191. Let $k, m, n \in \mathbb{Z}$. If $n|(km)$ and $\gcd(m, n) = 1$, then $n|k$.