A BEGINNING COURSE IN ARITHMETIC AND NUMBER THEORY

by

Lynne H. Walling

0

Preface

The problems herein are designed to lead the students through the process of deducing the rules of integer arithmetic (§1), patterns among certain sums of natural numbers (§2), the Euclidean algorithm, the Fundamental Theorem of Arithmetic, the fact that there are infinitely many primes (§3), and some results using congruences (§4). In §2 the students are introduced to the technique of induction, which is also used in §3 and §4.

We begin with very minimal assumptions, namely: We agree we understand what the natural numbers $1, 2, 3, 4, 5$, *etc.* represent. We also agree that, given a (finite) collection of objects, the number of objects we have does not depend on the order in which we count them. Also, we agree we understand what it means for one natural number to be larger or smaller than another.

When designing these problems, my intents were to change my role as instructor from "oracle" to "facilitator," to allow the students to work through the mathematics at their own pace and to discover things themselves, and to give them a clearer idea what it is we do as mathematicians – which is to deduce things and then to explain clearly our deductions.

One does not need to work through the material in the order in which the problems are organized, especially as doing so may be boring. However, when working problems from §2–4, one typically needs some results from §1. The instructor using this material can choose the amount of class time devoted to lecture, the amount of class time during which the students, individually or in groups, work through problems or present solutions. I perceive the greatest burden on the instructor to be the amount of time needed to read, listen and respond to the students' explanations. I strongly encourage instructors to have their students rewrite explanations when necessary or useful.

Many of these problems progress from specific examples to the general case. I recommend the students first work through the specific cases, get feedback from the instructor, then work through the first step generalizing the situation, get feedback, then work through the next generalization, get feed back, *etc.* I also believe it would be helpful to have each students take some of the correctly completed problems and prepare a (written or oral) presentation, identifying first the conclusion to be drawn, followed by an outline of the process, finishing with a thorough, clear and compelling series of deductions leading to the conclusion.

There is likely to be more than enough material here for a semester course. Please tell me of any typo's I have missed. Also, I appreciate all constructive remarks regarding these exercises. My email address is: walling@boulder.colorado.edu

A BEGINNING COURSE IN ARITHMETIC AND NUMBER THEORY

Instructions: You are encouraged to discuss your point of view with others **(including the instructor)** while you work on these assignment. Write clear, organized arguments, using complete sentences. If the instructions ever seem unclear or if you are stuck, ask the instructor for clarification or help. (Remember that you are encouraged to visit the instructor during office hours, and you are exhorted to make an appointment if you need to talk to the instructor but you cannot make it to office hours!)

Assumptions: We agree we understand what the numbers $1, 2, 3, 4, 5,$ *etc.* represent. (The latin abbreviation "*etc.*" indicates that the list extends indefinitely.) These numbers are called the *counting numbers*, since we use them to count things; they are also called the *natural numbers*, since they arise naturally in our lives. We also agree that, given a (finite) collection of objects, the number of objects we have does not depend on the order in which we count them. Also, we agree we understand what it means for one natural number to be larger or smaller than another.

§1. Rules of Arithmetic and Divisibility.

In this section we develop some basic rules of arithmetic.

A definition of addition: Imagine drawing 3 dots of one color followed by 5 dots of another color; we agree that $3 + 5$ is the total number of dots. More generally, let m and n represent natural numbers. Imagine drawing m dots of one color followed by n dots of another color; we agree that $m + n$ is the total number of dots.

Another assumption: We assume that when we add together two natural numbers, we obtain another natural number. For instance, $3 + 5$ is 8, which is another natural number.

1.1. In this exercise we want to establish that addition is "commutative;" that is, we want to explain why $3 + 5$ is the same as $5 + 3$. More generally, we want to explain why, given two natural numbers m and n, $m + n$ is the same as $n + m$. (So do not **assume** that addition is commutative; this is what we want to **deduce**!)

(a) On one line, draw 3 dots of one color, followed by 5 dots of another color. (So you have drawn $3 + 5$ dots.) Now turn your paper upside-down; thus you are looking at 5 dots of one color followed by 3 dots of another color, for a total of $5 + 3$ dots. Use this to explain why $3 + 5$ is the same as $5 + 3$.

(b) Follow the argument used in (a) to explain why $7 + 12$ is the same as $12 + 7$. Is it important here that the numbers are 7 and 12, or could this argument work with any two natural numbers?

(c) Let n represent a natural number. According to the above definition of addition, how can you describe the meaning of $3+n$? How can you describe the meaning of $n+3$? Do $3+n$ and $n+3$ represent the same quantities? Clearly explain your reasoning.

(d) Let m and n represent natural numbers. According to the above definition of addition, how can you describe the meaning of $m+n$? How can you describe the meaning of $n+m$? Do $m+n$ and $n+m$ represent the same quantities? Clearly explain your reasoning.

Notation: We sometimes use parentheses to indicate in which order to perform operations. For instance, the expression $(3+5)+9$ denotes the number we obtain by first adding 3 to 5, then adding 9 to the result. (So $(3+5)+9$ is the same as $8+9$.) Pictorially, $(3+5)+9$ denotes the number of dots we have when we have $3+5$ dots followed by 9 dots. Similarly, $3+(5+9)$ denotes the number we obtain by adding 3 to the number obtained by adding 5 to 9. (So $3+(5+9)$ is the same as $3+14$.) Pictorially, $3+(5+9)$ denotes the number of dots we have when we have 3 dots followed by $5+9$ dots.

1.2. In this exercise we want to establish that addition is "associative;" that is, we want to explain why $(3+5)+9$ represents the same quantity represented by $3+(5+9)$. More generally, with k, m and n denoting natural numbers, we want to explain why $(k+m)+n$ represents the same quantity represented by $k+(m+n)$. (So do not **assume** that addition is associative; this is what we want to **deduce**!)

(a) On one line, draw 17 dots. Draw a circle around the first $3+5$ dots. How many dots are outside the circle? Explain why this picture represents $(3+5)+9$ dots.

(b) Again, on one line, draw 17 dots. Draw a circle around the last $5+9$ dots. How many dots are outside the circle? Explain why this picture represents $3+(5+9)$ dots.

(c) Using (a) and (b), explain why $(3+5)+9$ represents the same number represented by $3+(5+9)$.

(d) Suppose n represents a natural number. How could you draw a picture representing $(3+5)+n$ dots? How could you draw a picture representing $3+(5+n)$ dots? Are there the same total number of dots in each picture? Explain your reasoning.

(e) Suppose m and n represent natural numbers. How could you draw a picture representing $(3+m)+n$ dots? How could you draw a picture representing $3+(m+n)$ dots? Are there the same total number of dots in each picture? Explain your reasoning.

(f) Suppose k, m and n represent natural numbers. How could you draw a picture representing $(k + m) + n$ dots? How could you draw a picture representing $k + (m + n)$ dots? Are there the same total number of dots in each picture? Explain your reasoning.

A definition of multiplication: The expression $5 \cdot 8$ refers to the quantity obtained by taking 5 copies of 8 objects. More generally, say m and n represent natural numbers; the expression $m \cdot n$ refers to the quantity obtained by taking m copies of n objects.

Another assumption: We assume that when we multiply together two natural numbers, we obtain another natural number. For instance, $5 \cdot 8$ is 40, another natural number.

1.3. For later convenience, we want a pictorial description of multiplication.

(a) Imagine 5 rows of dots, with 8 dots in each row. Using the above definition of multiplication, explain why the total number of dots is $5 \cdot 8$.

(b) Imagine 11 rows of dots, with 7 dots in each row. Using the above definition of multiplication, explain why the total number of dots is $11 \cdot 7$.

(c) Let n denote a natural number. Imagine 5 rows of dots, with n dots in each row. Using the above definition of multiplication, explain why the total number of dots is $5 \cdot n$.

(d) Let m and n denote natural numbers. Imagine m rows of dots, with n dots in each row. Using the above definition of multiplication, explain why the total number of dots is $m \cdot n$.

1.4. In this exercise we want to establish that multiplication is "commutative;" that is, we want to explain why $5 \cdot 8$ represents the same quantity as represented by $8 \cdot 5$. More generally, with m and n denoting natural numbers, we want to establish that $m \cdot n$ represents the same quantity as $n \cdot m$. (So do not **assume** that multiplication is commutative; this is what we want to **deduce**!)

(a) On a piece of paper, draw 5 rows of dots, with 8 dots in each row. Align the rows so that you have 8 columns of dots. (So the total number of dots is $5 \cdot 8$.) Now turn the paper sideways. How many rows of dots do you see? How many dots are in each row? Explain why this picture shows $8 \cdot 5$ dots; then explain why $5 \cdot 8$ represents the same quantity as $8 \cdot 5$.

(b) Clearly explain why $7 \cdot 3$ represents the same quantity as $3 \cdot 7$.

(c) Let m represent a natural number. Clearly explain why $m \cdot 8$ represents the same quantity as $8 \cdot m$.

(d) Let m and n represent natural numbers. Clearly explain why $m \cdot n$ represents the same quantity as $n \cdot m$.

Notation: The notation $(3 \cdot 5) \cdot 9$ refers to the quantity obtained by muliplying $3 \cdot 5$ by 9. (So $(3 \cdot 5) \cdot 9$ is the same as $15 \cdot 9$.) Similarly, $3 \cdot (5 \cdot 9)$ denotes the quantity obtained by multiplying 3 by the quantity $5 \cdot 9$. (So $3 \cdot (5 \cdot 9)$ is the same as $3 \cdot 45$.) More generally, with k, m and n denoting natural numbers, $(k \cdot m) \cdot n$ denotes the quantity obtained by multiplying the quantity $k \cdot m$ with n. Similarly, $k \cdot (m \cdot n)$ denotes the quantity obtained by multiplying k by the quantity $m \cdot n$.

1.5. In this exercise we want to establish that multiplication is "associative;" that is, we want to explain why $(3 \cdot 5) \cdot 8$ represents the same quantity as $3 \cdot (5 \cdot 8)$. More generally, with k, m and n representing natural numbers, we want to explain why $(k \cdot m) \cdot n$ represents the same quantity as $k \cdot (m \cdot n)$

(a) Take 3 small pieces of paper; on each piece, draw 5 rows of dots, with 7 dots in each row. Explain why the total number of dots on these 3 pieces of paper is $5 \cdot 21$. (**Suggestion:** Arrange the pieces of paper side by side, so that you see 5 rows of dots with 21 dots in each row.)

(b) As in (a), take 3 small pieces of paper; on each piece, draw 5 rows of dots, with 7 dots in each row. Explain why the total number of dots on these 3 pieces of paper is $15 \cdot 7$. Then using (a), explain why $5 \cdot 21$ is the same as $15 \cdot 7$.(**Suggestion:** Arrange the pieces of paper so that you see 15 rows of dots.)

(c) Let n be a natural number. Explain why $5 \cdot (3 \cdot n)$ is the same as $15 \cdot n$.

(d) Let k and n be natural numbers. Explain why $k \cdot (3 \cdot n)$ is the same as $(k \cdot 3) \cdot n$.

(e) Let k, m and n be natural numbers. Explain why $k \cdot (m \cdot n)$ is the same as $(k \cdot m) \cdot n$.

Remark: One can also show $k \cdot (m \cdot n)$ is the same as $(k \cdot m) \cdot n$ using a 3-dimensional argument, or by simply describing the sort of situation depicted in (a) in two different ways.

1.6. We want to explore the claim that "multiplication distributes over addition." Certainly $3 \cdot (2+5)$ is the same as $3 \cdot 2 + 3 \cdot 5$. (Here we agree that in the absence of any parentheses, we perform the multiplicative operations before we perform the additive operations; so to evaluate $3 \cdot 2 + 3 \cdot 5$, we first evaluate $3 \cdot 2$ and $3 \cdot 5$, and then we add together the two resulting numbers.)

(a) To help address the claim in question, create 3 rows of dots, each row containing $2 + 5$ (i.e. 7) dots. Now draw a vertical line so that 2 dots in each row are to the left of the line. What is the total number of dots to the left of the line? What is the total number of dots to the right of the line? Explain how this picture demonstrates that $3 \cdot (2 + 5)$ is equal to $3 \cdot 2 + 3 \cdot 5$. Explain your reasoning.

(b) Use a similar picture to show $6 \cdot (4 + 7)$ is the same as $6 \cdot 4 + 6 \cdot 7$.

(c) Use a similar picture to show $9 \cdot (11 + 15)$ is the same as $9 \cdot 11 + 9 \cdot 15$.

(d) Say k represents a natural number. Explain why $k \cdot (2+5)$ is the same as $k \cdot 2 + k \cdot 5$. (Suggestion: Modify your argument from (a).)

(e) Say k and m represent natural numbers. Explain why $k \cdot (m + 5)$ is the same as $k \cdot m + k \cdot 5$.

(f) Say k, m and n represent natural numbers. Explain why $k \cdot (m + n)$ is the same as $k \cdot m + k \cdot n$.

Notation: When two expressions denote the same quantity, we say they are equal. We use the symbol = to mean "is equal to."

1.7. Now we determine how to multiply together two sums.

(a) On a separate piece of paper, draw 5 rows, each with 5 dots. What is the total number of dots? Now draw a horizontal line so that 4 of the rows are above the line, and 1 of the rows below. Now draw a vertical line so that 4 columns of dots are to the left of the line, and 1 column is to the right. Using scissors, cut on your lines. Rearrange these four pieces of paper into 3 rectangles, so that one rectangle has 4 rows, each with 4 dots, one rectangle has 2 rows, each with 4 dots, and one rectangle has 1 row of one dot. How many dots are in each rectangle? Explain why this means

$$5 \cdot 5 = 4 \cdot 4 + 2 \cdot 4 + 1.$$

(b) Modify the argument used in (a) to deduce that

$$7 \cdot 7 = 6 \cdot 6 + 2 \cdot 6 + 1.$$

(c) Let n represent a natural number. Modify the argument used in (a) to deduce that for n a natural number,

$$(n + 1) \cdot (n + 1) = n \cdot n + 2 \cdot n + 1.$$

(Suggestion: Draw a picture.)

(d) Let m and n representa natural numbers. Modify the argument used in (a) to deduce that for n a natural number,

$$(n + m) \cdot (n + m) = n \cdot n + 2 \cdot (n \cdot m) + m \cdot m.$$

(Suggestion: Draw a picture.)

(e) On a separate piece of paper, draw 5 rows, each with 5 dots. What is the total number of dots? Now draw a horizontal line so that 3 of the rows are above the

line, and 2 of the rows below. Now draw a vertical line so that 1 column of dots are to the left of the line, and 4 columns are to the right. Using scissors, cut on your lines. (So you now have 4 rectangles.) How many dots are in each rectangle? Explain why this means

$$(3+2)\cdot(1+4) = 3\cdot 1 + 2\cdot 1 + 3\cdot 4 + 2\cdot 4.$$

(f) Use the method of (e) to deduce that

$$(3+5)\cdot(2+4) = 3\cdot 2 + 5\cdot 2 + 3\cdot 4 + 5\cdot 4.$$

(Suggestion: Begin by drawing $(3+5)$ rows, each with $(2+4)$ dots.)

(g) Use the ideas used in (e) to deduce that, for k a natural number,

$$(k+5)\cdot(2+4) = k\cdot 2 + k\cdot 4 + 5\cdot 2 + 5\cdot 4.$$

(Suggestion: Draw a picture.)

(h) Use the ideas used in (e) to deduce that, for k and m natural numbers,

$$(k+5)\cdot(m+4) = k\cdot m + k\cdot 4 + 5\cdot m + 5\cdot 4.$$

(i) Use the ideas used in (e) to deduce that, for k, m and n natural numbers,

$$(k+n)\cdot(m+4) = k\cdot m + k\cdot 4 + n\cdot m + n\cdot 4.$$

(j) Use the ideas used in (e) to deduce that, for k, m, n and t natural numbers,

$$(k+n)\cdot(m+t) = k\cdot m + k\cdot t + n\cdot m + n\cdot t.$$

Terminology: Since $24 = 6\cdot 4$, we say 24 is divisible by 6. We also say that 6 divides 24, and that 6 is a divisor of 24. Similarly, since $27 = 9\cdot 3$, we say 27 is divisible by 9, and 9 is a divisor of 27. More generally, when n is a natural number that is equal to 6 times another natural number (i.e.

$$n = 6\cdot k$$

for some natural number k), we say that n is divisible by 6 and that 6 is a divisor of n. More generally still, when m and n are natural numbers and n is equal to m times another natural number (i.e.

$$n = m\cdot k$$

for some natural number k), we say that n is divisible by m and that m is a divisor of n. Notice that the equation $n = m \cdot k$ means n objects can be partitioned into m groups, each with k objects. Equivalently, since $m \cdot k = k \cdot m$, the equation $n = m \cdot k$ means n objects can be partitioned into k groups, each with m objects.

1.8. We want to compare the size of a natural number to the size of one of its divisors.

(a) Certainly 10 is a natural number that is divisible by 2. How do 10 and 2 compare in size? (That is, which is larger/smaller?) Explain your reasoning, using complete sentences. (Suggestion: Imagine partitioning 10 objects into groups of 2.)

(b) Also, 18 is a natural number that is divisible by 2. How do 18 and 2 compare in size? Explain your reasoning, using complete sentences.

(c) Suppose n is a natural number that is divisible by 2. How do n and 2 compare in size? Explain your reasoning, using complete sentences. (Note that n could be 2, since $2 = 2 \cdot 1$. Also, remember that the assumption that n is divisible by 2 means n objects can be partitioned into groups of 2.)

(d) Suppose n is a natural number that is divisible by 3. How do n and 3 compare in size? Explain your reasoning, using complete sentences.

(e) Suppose n is a natural number that is divisible by 10. How do n and 10 compare in size? Explain your reasoning, using complete sentences.

(f) Suppose n is a natural number that is divisible by m. How do n and m compare in size? Justify your answer, using complete sentences.

1.9. (a) Suppose that b is a natural number that is divisible by 5. Is $5 + b$ divisible by 5? If so, explain why $5 + b$ satisfies the definition of divisibility by 5; if not, explain why not. (You may want to use your result from #1.6 (f).)

(b) Suppose still that b is a natural number that is divisible by 5. Is $10 + b$ divisible by 5? If so, explain why $10 + b$ satisfies the definition of divisibility by 5; if not, explain why not.

(c) Suppose still that b is a natural number that is divisible by 5. Is $15 + b$ divisible by 5? If so, explain why $15 + b$ satisfies the definition of divisibility by 5; if not, explain why not.

(d) Suppose that a and b are natural numbers, each of which is divisible by 5. Is $a + b$ divisible by 5? If so, explain why $a + b$ satisfies the definition of divisibility by 5; if not, explain why not.

(e) Suppose that a, b and c are natural numbers, and suppose that each a and b is divisible by c. Is $a + b$ divisible by c? If so, explain why $a + b$ satisfies the

definition of divisibility by c; if not, explain why not.

A definition of subtraction: Suppose we have 5 objects, then we subtract, or remove, or eliminate, 3 of these objects; the remaining number of objects is denoted by $5-3$. Pictorially, imagine drawing 5 dots, then crossing out 3 dots; the remaining number of dots is $5-3$. More generally, suppose we have n objects where n is a natural number at least as big as 3, and then we remove 3 of the objects; the remaining number of ojects is $n-3$. Pictorially, suppose we draw n dots and then we cross out 3 dots; the remaining number of dots is $n-3$. More generally still, suppose we have n objects, where n is a natural number, and then we remove k of the objects where k is a natural number not exceeding n; the remaining number of objects is $n-k$.

Another assumption: Suppose k and n are natural numbers, and suppose k is smaller than n. Then we assume that $n-k$ is another natural number. For instance, 5 and 3 are natural numbers and 3 is smaller than 5; $5-3$ is 2, which is another natural number.

1.10. We want to explore the claim that "multiplication distributes over subtraction." Certainly $3\cdot(7-2) = 15 = 3\cdot 7 - 3\cdot 2$. (Here we agree that in the absence of any parentheses, we perform the multiplication before we perform the subtraction; so to evaluate $3\cdot 7-3\cdot 2$, we first evaluate $3\cdot 7$ and $3\cdot 2$, and then we subtract $3\cdot 2$ from $3\cdot 7$.) More generally, for k, m, n natural numbers with m at least as large as n, we want to show that

$$k\cdot(m-n) = k\cdot m - k\cdot n.$$

(a) Draw 3 rows, each with 7 dots. Then in each row, cross out the last 2 dots. Explain why your picture now represents $3\cdot(7-2)$ dots. (Recall how we defined multiplication.) Now draw a vertical line so that the crossed out dots are to the right of the line and the other dots are to the left. Explain why this picture represents $3\cdot 7-3\cdot 2$.

(b) Let k be a natural number. Explain why $k\cdot(7-2) = k\cdot 7 - k\cdot 2$.

(c) Let k, m be natural numbers with m at least 2. Explain why $k\cdot(m-2) = k\cdot m - k\cdot 2$.

(d) Let k, m, n be natural numbers with m at least n. Explain why $k\cdot(m-n) = k\cdot m - k\cdot n$.

1.11. (a) Suppose m is a natural number, and suppose $m+12$ is divisible by 3. Explain why this means m is divisible by 3. (We can show m is divisible by 3 by showing that m objects can be partitioned into groups of 3. Given $m+12$ objects, can these be partitioned into groups of 3? If so, why? How many groups give us 12 objects? Removing these 12 objects, with what are we left?)

(b) Suppose m is a natural number, and suppose $m + 12$ is divisible by 6. Explain why this means m is divisible by 6.

(c) Suppose m and n are natural numbers, and suppose n and $m+n$ are each divisible by 3. Explain why this means m is divisible by 3.

(d) Suppose m, n and d are natural numbers, and suppose n and $m + n$ are each divisible by d. Explain why this means m is divisible by d.

1.12. (a) Define "zero".

(b) When we have a line with 5 dots, what is the largest number of dots we can cross out? How many dots would then be left?

(c) Say m and n represent quantities and n is at least as large as m. When is $n - m$ equal to zero? Briefly explain your reasoning.

(d) Using your definition of zero, explain why $0 \cdot 5$ and $5 \cdot 0$ should be zero; here 0 represents zero. (You may want to use our definition of multiplication for this.) More generally, letting n represent any natural number, explain why $0 \cdot n$ and $n \cdot 0$ should be zero.

Definition: We say a number is a whole number if it is a natural number or zero. So the whole numbers are $0, 1, 2, 3, \ldots$.

(e) Say m and n are whole numbers, and $m \cdot n = 0$. Clearly explain why either m or n (or both) must be zero.

1.13. (a) Draw 9 dots, then draw one circle around 5 of these dots. Within this circle, draw one circle around 3 dots. (So $5 - 3$ dots are in the big circle but not in the small circle.) Now cross out the dots in the big circle but not in the small circle. Explain why the number of dots not crossed out is $9 - (5 - 3)$.

(b) Using ink, draw 9 dots, then draw one circle around 5 of these dots. Within that circle, draw one circle around 3 dots. Using a pencil, cross out the dots in the big circle; this leaves you with $9 - 5$ dots not crossed out. Now erase the cross marks on the dots inside the small circle; so now you have $(9 - 5) + 3$ dots not crossed out. Does this picture look the same as your picture created in (a)? Can you conclude that $9 - (5 - 3)$ is the same as $(9 - 5) + 3$? Briefly explain your reasoning.

(c) Let a, b and c denote natural numbers with a larger than b, and b larger than c. Imagine drawing a dots; describe a process that leaves you with $a - (b - c)$ dots not crossed out. Explain your reasoning. (You may want to mimic the procedure used in (a).)

(d) Again, let a, b and c denote natural numbers with a larger than b, and b larger than c. Imagine drawing a dots; describe a process that leaves you with $(a-b)+c$ dots not crossed out. Explain your reasoning. (You may want to mimic the procedure used in (b).)

(e) Again, let a, b and c denote natural numbers with a larger than b, and b larger than c. Using (c) and (d), compare the quantities $a-(b-c)$ and $(a-b)+c$; explain your reasoning.

Terminology: The numbers

$$0, 1, -1, 2, -2, 3, -3, 4, -4, 5, -5, \ldots$$

are called the integers. The numbers

$$-1, -2, -3, -4, -5, \ldots$$

are called the negative integers.

More assumptions: Negative numbers are often useful to express orientation, i.e. to distinguish forward from reverse. We interpret the symbol $-$ to mean "in reverse." So for instance, imagine being on a very long, straight path where a forward direction is indicated. To take 5 steps, we move forward 5 steps. To take -5 steps, we move **in reverse** 5 steps (so we move **backward** 5 steps). Notice that when you take 7 steps then -3 steps (i.e. when you move forward 7 steps then backward 3 steps), then you are in the same place as when you take -3 steps then 7 steps. Similarly, when you take 5 steps then -12 steps, then you are in the same place as when you take -12 steps then 5 steps. More generally, we assume that, for x and y integers, when you take x steps then y steps, you are in the same place as when you take y steps then x steps. So we are assuming addition of integers is commutative, i.e. $x+y=y+x$ for any integers x and y. Also, when you take $\big(7+(-3)\big)$ steps followed by 5 steps, you are in the same place as when you take 7 steps followed by $\big((-3)+5\big)$ steps. More generally, we assume that addition of integers is associative, i.e. $(x+y)+z=x+(y+z)$ for any integers x, y and z.

1.14. Throughout, let k and m represent natural numbers.

(a) After taking $7+(-3)$ steps, have you moved forward or backward? How many steps forward or backward are you from where you started? Deduce that $7+(-3)=7-3$. (To take $7-3$ steps, what do you do? How does "backward" compare to "eliminating"?)

(b) Suppose k is smaller than 7. After taking $7+(-k)$ steps, have you moved forward or backward? How many steps forward or backward are you from where you started? Deduce that $7 + (-k) = 7 - k$. (To take $7 - k$ steps, what do you do?)

(c) Suppose k is smaller than m. After taking $m + (-k)$ steps, have you moved forward or backward? How many steps forward or backward are you from where you started? Deduce that $m + (-k) = m - k$. (To take $m - k$ steps, what do you do?)

1.15. Here we establish that multiplication of integers is commutative. Throughout, let k and m represent natural numbers.

(a) Recall that to draw $3 \cdot 7$ dots, we draw 3 copies of 7 dots. So we repeat the process of drawing 7 dots, doing this 3 times. So to take $3 \cdot 7$ steps, we repeat the process of moving forward 7 steps, doing so 3 times. Thus to take $3 \cdot (-7)$ steps, we repeat the process of moving **in reverse** 7 steps, doing so 3 times. When we do this, how many steps backward do we take? Explain why this means $3 \cdot (-7) = -21$. (To take -21 steps, what do you do?)

(b) Similarly, to take $k \cdot (-7)$ steps, we repeat the process of moving **in reverse** 7 steps, doing so k times. When we do this, how many steps backward do we take? Deduce that $k \cdot (-7) = -(k \cdot 7)$. (To take $-(k \cdot 7)$ steps, what do you do?)

(c) Similarly, to take $k \cdot (-m)$ steps, we repeat the process of moving **in reverse** m steps, doing so k times. When we do this, how many steps backward do we take? Explain why this means $k \cdot (-m) = -(k \cdot m)$. (To take $-(k \cdot m)$ steps, what do you do?)

(d) Using the symbol $-$ to denote "in reverse," to take $(-7) \cdot 3$ steps, we repeat the process of moving forward 3 steps, doing so **in reverse** 7 times. So when we take $(-7) \cdot 3$ steps, do we move forward or backward? How many steps forward or backward do we move? Briefly but clearly explain your reasoning. Deduce that $(-7) \cdot 3 = -21$.

(e) To take $(-7) \cdot k$ steps, we repeat the process of moving forward k steps, doing so **in reverse** 7 times. So when we take $(-7) \cdot k$ steps, do we move forward or backward? How many steps forward or backward do we move? Briefly but clearly explain your reasoning. Deduce that $(-7) \cdot k = -(7 \cdot k)$.

(f) To take $(-m) \cdot k$ steps, we repeat the process of moving forward k steps, doing so **in reverse** m times. So when we take $(-m) \cdot k$ steps, do we move forward or backward? How many steps forward or backward do we move? Briefly but clearly explain your reasoning. Deduce that $(-m) \cdot k = -(m \cdot k)$.

(g) Use the fact that $k \cdot m = m \cdot k$ and your results from (c) and (f) to deduce that $k \cdot (-m) = (-m) \cdot k$.

(h) Again we use the symbol $-$ to denote "in reverse." So to take $(-3) \cdot (-7)$ steps, we repeat the process of moving **in reverse** 7 steps, doing so **in reverse** 3 times. So when we take $(-3) \cdot (-7)$ steps, do we move forward or backward? How many steps forward or backward do we move? Briefly but clearly explain your reasoning. Then explain why this means $(-3) \cdot (-7) = 21$.

(i) To take $(-3) \cdot (-m)$ steps, we repeat the process of moving **in reverse** m steps, doing so **in reverse** 3 times. So when we take $(-3) \cdot (-m)$ steps, do we move forward or backward? How many steps forward or backward do we move? Briefly but clearly explain your reasoning. Then deduce that $(-3) \cdot (-m) = 3 \cdot m$.

(j) To take $(-k) \cdot (-m)$ steps, we repeat the process of moving **in reverse** m steps, doing so **in reverse** k times. So when we take $(-k) \cdot (-m)$ steps, do we move forward or backward? How many steps forward or backward do we move? Briefly but clearly explain your reasoning. Then explain why this means $(-k) \cdot (-m) = k \cdot m$. Similarly, explain why $(-m) \cdot (-k) = m \cdot k$.

(k) Recall that we already know that $k \cdot m = m \cdot k$. Use this and your results from (j) to deduce that $(-k) \cdot (-m) = (-m) \cdot (-k)$.

Terminology: We say that 3 divides -12 (or equivalently, that 3 is a divisor of -12 or that -12 is divisible by 3) since $-12 = 3 \cdot (-4)$. More generally, we say that 3 divides an integer n if $n = 3 \cdot q$ for some integer q. More generally still, we say that an integer m divides another integer n if $n = m \cdot q$ for some integer q.

1.16. We want to establish that multiplication of integers is associative. (Recall that we know multiplication of natural numbers is associative.) We describe here an algebraic approach, although one could also use a geometric approach.

(a) Briefly explain why $(-3) \cdot 4 = -12 = -(3 \cdot 4)$, and why $(-12) \cdot 7 = -(12 \cdot 7)$. (Suggestion: Use #1.15 (f).)

(b) Briefly explain why $(-3) \cdot 28 = -(3 \cdot 28)$. Deduce that $(-3) \cdot \big(4 \cdot 7\big) = -\big(3 \cdot (4 \cdot 7)\big)$. Explain why $\big((-3) \cdot 4\big) \cdot 7 = (-3) \cdot \big(4 \cdot 7\big)$. (Suggestion: Use (a) and #1.5.)

(c) Let n represent a natural number. Briefly explain why $(-3) \cdot 4 = -(3 \cdot 4)$, and why $(-12) \cdot n = -(12 \cdot n)$.

(d) Again, let n represent a natural number. Briefly explain why $(-3) \cdot \big(4 \cdot n\big) = -\big(3 \cdot (4 \cdot n)\big)$. Deduce that $(-3) \cdot \big(4 \cdot n\big) = -\big(3 \cdot (4 \cdot n)\big)$. Now explain why $\big((-3) \cdot 4\big) \cdot n = (-3) \cdot \big(4 \cdot n\big)$.

(e) Let m and n represent natural numbers. Briefly explain why $(-3)\cdot m = -(3\cdot m)$, and why $\big(-(3\cdot m)\big)\cdot n = -\big((3\cdot m)\cdot n\big)$.

(f) Again, let m and n represent natural numbers. Briefly explain why $(-3)\cdot\big(m\cdot n\big) = -\big(3\cdot(m\cdot n)\big)$. Deduce that $(-3)\cdot\big(m\cdot n\big) = -\big(3\cdot(m\cdot n)\big)$. Now explain why $\big((-3)\cdot m\big)\cdot n = (-3)\cdot\big(m\cdot n\big)$.

(g) Let k, m and n represent natural numbers. Briefly explain why $(-k)\cdot m = -(k\cdot m)$, and why $\big(-(k\cdot m)\big)\cdot n = -\big((k\cdot m)\cdot n\big)$.

(h) Again, let k, m and n represent natural numbers. Briefly explain why $(-k)\cdot\big(m\cdot n\big) = -\big(k\cdot(m\cdot n)\big)$. Deduce that $(-k)\cdot\big(m\cdot n\big) = -\big(k\cdot(m\cdot n)\big)$. Now explain why $\big((-k)\cdot m\big)\cdot n = (-k)\cdot\big(m\cdot n\big)$.

(i) Let k, m and n represent natural numbers. Explain why $\big((-k)\cdot(-m)\big)\cdot n = (-k)\cdot\big((-m)\cdot n\big)$.

(j) Let k, m and n represent natural numbers. Explain why $\big((-k)\cdot(-m)\big)\cdot(-n) = (-k)\cdot\big((-m)\cdot(-n)\big)$.

(k) Let k, m and n represent natural numbers. Explain why $\big((-k)\cdot m\big)\cdot(-n) = (-k)\cdot\big(m\cdot(-n)\big)$.

(l) Let k, m and n represent natural numbers. Explain why $\big(k\cdot(-m)\big)\cdot n = k\cdot\big((-m)\cdot n\big)$.

(m) Let k, m and n represent natural numbers. Explain why $\big(k\cdot(-m)\big)\cdot(-n) = k\cdot\big((-m)\cdot(-n)\big)$.

(n) Let k, m and n represent natural numbers. Explain why $\big(k\cdot m\big)\cdot(-n) = k\cdot\big(m\cdot(-n)\big)$.

1.17. Recall that for k, m and n natural numbers, $k\cdot(m+n) = k\cdot m + k\cdot n$. We establish that with x, y and z integers, $x\cdot(y+z) = x\cdot y + x\cdot z$.

(a) To take $3\cdot\big(5+(-7)\big)$ steps, you repeat 3 times the process of moving forward 5 steps then backward 7 steps. Altogether, how many steps forward to you move? How many steps backward do you move?

(b) To take $3\cdot 5 + 3\cdot(-7)$ steps, you repeat 3 times the process of moving forward 5 steps, then you repeat 3 times the process of moving backward 7 steps. Altogether, how many steps forward to you move? How many steps backward do you move? Using (a), explain why $3\cdot\big(5+(-7)\big) = 3\cdot 5 + 3\cdot(-7)$.

(c) Suppose k, m and n are natural numbers. Explain why $k\cdot\big(m+(-n)\big) = k\cdot m + k\cdot(-n)$. (Suggestion: Mimic your arguments from (a) and (b).)

(d) Suppose k, m and n are natural numbers. Explain why $k\cdot\big((-m)+(-n)\big) =$

$k \cdot (-m) + k \cdot (-n)$.

(e) Suppose k, m and n are natural numbers. Explain why $k \cdot \big((-m) + n\big) = k \cdot (-m) + k \cdot n$.

(f) Suppose k, m and n are natural numbers. Explain why $(-k) \cdot \big(m + n\big) = (-k) \cdot m + (-k) \cdot n$.

(g) Suppose k, m and n are natural numbers. Explain why $(-k) \cdot \big((-m) + n\big) = (-k) \cdot (-m) + (-k) \cdot n$.

(h) Suppose k, m and n are natural numbers. Explain why $(-k) \cdot \big(m + (-n)\big) = (-k) \cdot m + (-k) \cdot (-n)$.

(i) Suppose k, m and n are natural numbers. Explain why $(-k) \cdot \big((-m) + (-n)\big) = (-k) \cdot (-m) + (-k) \cdot (-n)$.

§2: Looking for patterns.

Terminology: We call a natural number even when it is divisible by 2. The odd natural numbers are those not divisible by 2. So the odd natural numbers are between the even natural numbers, and thus each even natural number is preceded by an odd natural number.

2.1. (a) By definition, the 1st even natural number is $2 = 1 \cdot 2$.
The next even natural number is $2 + 2 = 4$, so the 2nd even natural number is $4 = 2 \cdot 2$.
The next even natural number is $4 + 2 = 6$, so the 3rd even natural number is $6 = 3 \cdot 2$.
The next even natural number is $6 + 2 = 8$, so the 4th even natural number is $8 = 4 \cdot 2$.
What is the 5th even natural number?
What is the 6th even natural number?
What is the 10th even natural number?
What is the 25th even natural number?
What is the 40th even natural number?
What is the nth even natural number? (Your answer may be in terms of n.)
What is the $(n+1)$st even natural number? (Once again, your answer may be in terms of n. Also, you can check your formula for $n = 1$, $n = 2$, $n = 3$, $n = 4$ and $n = 5$.)

(b) By definition, the 1st odd natural number is $1 = 1 \cdot 2 - 1$.
The 2nd odd natural number is $3 = 2 \cdot 2 - 1$.
The 3rd odd natural number is $5 = 3 \cdot 2 - 1$.
The 4th odd natural number is $7 = 4 \cdot 2 - 1$.
What is the 5th odd natural number?
What is the 6th odd natural number?
What is the 10th odd natural number?
What is the 25th odd natural number?
What is the 40th odd natural number?
What is the nth odd natural number?
What is the $(n + 1)$st odd natural number? (You can check your formula for $n = 1$, $n = 2$, $n = 3$, $n = 4$ and $n = 5$.)

(c) Evaluate $1^2 = 1 \cdot 1$, $2^2 = 2 \cdot 2$, $3^2 = 3 \cdot 3$, $4^2 = 4 \cdot 4$, $5^2 = 5 \cdot 5$.

(d) Evaluate $1 + 3$, the sum of the first 2 odd natural numbers.
Evaluate $1 + 3 + 5$, the sum of the first 3 odd natural numbers.

Evaluate the sum of the first 4 odd natural numbers.

Evaluate the sum of the first 5 odd natural numbers.

(e) We now consider whether there is a pattern here: Given your computations in (c) and (d), guess the value of the sum of the first 6 odd natural numbers. (You can easily check whether your guess in correct.)

Guess the value of the sum of the first 7 odd natural numbers.

Guess the value of the sum of the first 10 odd natural numbers.

Guess the value of the sum of the first 25 odd natural numbers.

Guess the value of the sum of the first 40 odd natural numbers.

Guess the value of the sum of the first 100 odd natural numbers.

Guess the value of the sum of the first n odd natural numbers.

Guess the value of the sum of the first $(n+1)$ odd natural numbers.

(f) You just guessed the value of the sum of the first n odd natural numbers; verify your guess is correct for $n = 2$, for $n = 3$, for $n = 4$, and for $n = 5$. (If you find your guess is not correct for one of these values of n, modify your guess!)

Imagine a stairway to heaven. Of course, it has infinitely many steps. Still, you can climb the stairway if you know:

(i) how to get to the 1st step, and

(ii) how to get from one step to the next.

So once you get to the 1st step, you can get to the 2nd step. Once you get to the 2nd step, you can get to the 3rd step. Once you get to the 3rd step, you can get to the 4th step; and so on.

To determine whether your formula for the sum of the first n odd natural numbers is correct, we follow a similar procedure.

(g) Suppose your formula for the sum of the first n odd natural numbers is correct. We want to know whether this implies your formula for the sum of the first $(n+1)$ odd natural numbers is also correct. Briefly explain why [the sum of the first n odd natural numbers] + [the (n+1)st odd natural number] gives us the sum of the first $(n+1)$ odd natural numbers. Now using your previous formulas, evaluate

[the sum of the first n odd natural numbers]

$+$ [the $(n+1)$st odd natural number].

Does this agree with your guess of the value of the sum of the first $(n+1)$ odd natural numbers?

(h) Explain why (g) does **not** imply that your guess of the value of the sum of the first $(n+1)$ odd natural numbers is correct. Explain why (g) does imply that **if** your guess of the value of the sum of the first n odd natural numbers is correct **then** your guess of the value of the sum of the first $(n+1)$ odd natural numbers is correct.

(i) In (d) you evaluated the sum of the first 5 odd natural numbers. Also, we know that **if** your guess of the value of the sum of the first n odd natural numbers is correct **then** your guess of the value of the sum of the first $(n+1)$ odd natural numbers is correct. What does this say when $n = 5$? Since you know your formula for the sum of the first n odd natural numbers is correct when $n = 5$, what can you conclude?

(j) We know that **if** your guess of the value of the sum of the first n odd natural numbers is correct **then** your guess of the value of the sum of the first $(n+1)$ odd natural numbers is correct. Does the hypothesis hold for $n = 6$? What can you then conclude?

(k) We know that **if** your guess of the value of the sum of the first n odd natural numbers is correct **then** your guess of the value of the sum of the first $(n+1)$ odd natural numbers is correct. Does the hypothesis hold for $n = 7$? What can you then conclude?

(l) We know that **if** your guess of the value of the sum of the first n odd natural numbers is correct **then** your guess of the value of the sum of the first $(n+1)$ odd natural numbers is correct. Does the hypothesis hold for $n = 8$? What can you then conclude?

(m) We know that **if** your guess of the value of the sum of the first n odd natural numbers is correct **then** your guess of the value of the sum of the first $(n+1)$ odd natural numbers is correct. Does the hypothesis hold for $n = 9$? What can you then conclude?

(n) Explain how your computations in (c), (d) and (g) allow you to conclude that, for each successive value of n, your formula for the sum of the first n odd natural numbers is correct.

(o) (**Geometric argument:**) This pattern can also be deduced using a geometric argument. Begin with a picture of one dot. To expand this to a picture of two rows, each with two dots, how many dots need to be introduced to your picture? To expand the resulting picture to one with three rows, each with 3 dots, how many dots need to be introduced to your picture? Suppose you have n rows,

each with n dots; to expand the picture to one with $(n+1)$ rows, each with $(n+1)$ dots, how many dots need to be introduced to your picture? Clearly and thoroughly explain your reasoning, then use this to give another explanation for the implication stated in (h).

2.2. We now consider the sum of the first n even integers.

(a) Evaluate $2+4$, the sum of the first 2 even natural numbers.
Evaluate $2+4+6$, the sum of the first 3 even natural numbers.
Evaluate the sum of the first 4 even natural numbers.
Evaluate the sum of the first 5 even natural numbers. Also, evaluate the expressions $2 \cdot 3,\ 3 \cdot 4,\ 4 \cdot 5,\ 5 \cdot 6$.

(b) We now consider whether there is a pattern here: Given your computations in (a), guess the value of the sum of the first 6 even natural numbers. (You can easily check whether your guess in correct.)
Guess the value of the sum of the first 7 even natural numbers.
Guess the value of the sum of the first 10 even natural numbers.
Guess the value of the sum of the first 25 even natural numbers.
Guess the value of the sum of the first 40 even natural numbers.
Guess the value of the sum of the first 100 even natural numbers.
Guess the value of the sum of the first n even natural numbers.
Guess the value of the sum of the first $(n+1)$ even natural numbers.

(c) You just guessed the value of the sum of the first n even natural numbers; verify your guess is correct for $n=2$, for $n=3$, for $n=4$, and for $n=5$. (If you find your guess is not correct for one of these values of n, modify your guess!)

(d) Suppose your formula for the sum of the first n even natural numbers is correct. We want to know whether this implies your formula for the sum of the first $(n+1)$ even natural numbers is correct. Briefly explain why the sum of the first n even natural numbers $+$ the $(n+1)$st even natural number gives you the sum of the first $(n+1)$ even natural numbers. Using your assumption and your previous formulas, evaluate

$$[\text{the sum of the first } n \text{ even natural numbers}]$$

$$+ \quad [\text{the } (n+1)\text{st even natural number}].$$

Does this agree with your guess for the value of the sum of the first $(n+1)$ even natural numbers?

(e) Explain why (d) does **not** imply that your guess of the value of the sum of the first $(n+1)$ even natural numbers is correct, but (d) does imply that **if** your guess of the value of the sum of the first n even natural numbers is correct **then** your guess of the value of the sum of the first (n_1) even natural numbers is correct.

(f) In (a) you evaluated the sum of the first 5 even natural numbers. Also, we know that **if** your guess of the value of the sum of the first n even natural numbers is correct **then** your guess of the value of the sum of the first $(n+1)$ even natural numbers is correct. What does this say when $n = 5$? Since you know your formula for the sum of the first n even natural numbers is correct when $n = 5$, what can you conclude?

(g) We know that **if** your guess of the value of the sum of the first n even natural numbers is correct **then** your guess of the value of the sum of the first $(n+1)$ even natural numbers is correct. Does the hypothesis hold for $n = 6$? What can you then conclude?

(h) We know that **if** your guess of the value of the sum of the first n even natural numbers is correct **then** your guess of the value of the sum of the first $(n+1)$ even natural numbers is correct. Does the hypothesis hold for $n = 7$? What can you then conclude?

(i) We know that **if** your guess of the value of the sum of the first n even natural numbers is correct **then** your guess of the value of the sum of the first $(n+1)$ even natural numbers is correct. Does the hypothesis hold for $n = 8$? What can you then conclude?

(j) We know that **if** your guess of the value of the sum of the first n even natural numbers is correct **then** your guess of the value of the sum of the first $(n+1)$ even natural numbers is correct. Does the hypothesis hold for $n = 9$? What can you then conclude?

(k) Explain how your computations in (c), (d) and (g) allow you to conclude that, for each successive value of n, your formula for the sum of the first n even natural numbers is correct.

(l) Find a geometric argument that shows your formula for the sum of the first n even integers is correct.

2.3. Consider the following arrangement of stars:

```
*
* *
* * *
```

There are a total of $1+2+3$ stars, and they are arranged to form a triangle. For this reason, $1+2+3$ is called a triangular number. Similarly, $1+2+3+4$ is called a triangular number.

*

* *

* * *

* * * *

Terminology: We define the triangular numbers as follows.

Let $T_1 = 1 =$ the first triangular number,
let $T_2 = 1+2 =$ the second triangular number,
let $T_3 = 1+2+3 =$ the third triangular number,
let $T_4 = 1+2+3+4 =$ the fourth triangular number,
let $T_5 = 1+2+3+4+5 =$ the fifth triangular number,
and so on. So for n a natural number, T_n denotes the nth triangular number, which is the sum of the first n natural numbers.

(a) Compute the values of T_1+T_2, T_2+T_3, T_3+T_4, T_4+T_5, and T_5+T_6. Does this list look familiar? (You may want to compare this list the one you created in #2.1 (c).)

(b) Without performing the computation, what would you guess T_6+T_7 is? Without performing the computation, what would you guess T_7+T_8 is? Without performing the computation, what would you guess T_8+T_9 is? What would you guess $T_{25}+T_{26}$ is? What would you guess $T_{40}+T_{41}$ is? What would you guess $T_{100}+T_{101}$ is?

(c) Given a natural number n, what would you guess $T_{(n-1)}+T_n$ is? (You can check your guess for $n=2$, $n=3$, $n=4$, $n=5$ and $n=6$.) What would you guess $T_n+T_{(n+1)}$ is? (You can check your guess for$n+1$, $n=2$, $n=3$, $n=4$ and $n=5$.)

(d) Notice that $T_2 = 1+2 = T_1+2$, $T_3 = \big(1+2\big)+3 = T_2+3$, $T_4 = \big(1+2+3\big)+4 = T_3+4$, and so on. More generally, for n a natural number, T_n =(the sum of the first $(n-1)$ natural numbers)$+n = T_{(n-1)}+n$. Briefly explain why $T_{(n+1)} = T_n+(n+1)$. So

$$(*) \qquad T_n+T_{(n+1)} = \big(T_{(n-1)}+n\big)+\big(T_n+(n+1)\big)\,.$$

If your guess for the value of $T_{(n-1)}+T_n$ is correct, then is your guess for $T_n+T_{(n+1)}$ correct? (Use the equation labeled (*) together with (c).)

(e) Explain why (d) does **not** imply that your guess of the value of $T_n + T_{(n+1)}$ is correct, but (d) does imply that **if** your guess for the value of $T_{(n-1)} + T_n$ is correct **then** your guess for the value of $T_n + T_{(n+1)}$ is correct.

(f) In (a) you evaluated $T_5 + T_6$. Use the conclusion of (d) (as described in (e)) with $n = 6$ to verify that your guess for $T_6 + T_7$ is correct.

(g) From (f) you know that your guess for $T_6 + T_7$ is correct. Use the conclusion of (d) with $n = 7$ to verify that your guess for $T_7 + T_8$ is correct.

(h) From (g) you know that your guess for $T_7 + T_8$ is correct. Use the conclusion of (d) with $n = 8$ to verify that your guess for $T_8 + T_9$ is correct.

(i) Explain how your computations in (a) and (d) allow you to conclude that, for each successive value of n, your formula for $T_n + T_{(n+1)}$ is correct.

(j) Find a geometric argument that shows your formula for $T_n + T_{(n+1)}$ is correct.

Notation: When a natural number n is even, we write $\frac{1}{2} \cdot n$ to denote half of n. For instance, $\frac{1}{2} \cdot 6 = 3$, and $\frac{1}{2} \cdot 10 = 5$. More generally, if n is even then $n = 2 \cdot k$ for some natural number k; then

$$\frac{1}{2} \cdot n = k.$$

2.4. We now find a formula for T_n, the nth triangular number. (Recall that T_n is the sum of the first n natural numbers.)

(a) Suppose you have two consecutive natural numbers. Explain why one of these numbers is even and the other is odd.

(b) Let n be a natural number; so the next natural number is $(n + 1)$. Using (a), explain why $n \cdot (n + 1)$ is even, and so $\frac{1}{2} \cdot n \cdot (n + 1)$ is a natural number.

(c) Compute the values of T_1, T_2, T_3, T_4 and T_5. Also, compute the values of $\frac{1}{2} \cdot 1 \cdot 2$, $\frac{1}{2} \cdot 2 \cdot 3$, $\frac{1}{2} \cdot 3 \cdot 4$, $\frac{1}{2} \cdot 4 \cdot 5$, and $\frac{1}{2} \cdot 5 \cdot 6$. What would you guess is the value of T_6? What would you guess is the value of T_7? What would you guess is the value of T_{10}? What would you guess is the value of T_{25}? What would you guess is the value of T_{40}? What would you guess is the value of T_{100}? With n a natural number, what would you guess is the value of T_n? (You can check your guess for $n = 1$, $n = 2$, $n = 3$, $n = 4$ and $n = 5$.) What would you guess is the value of $T_{(n+1)}$? (You can check your guess for $n = 1$, $n = 2$, $n = 3$ and $n = 4$.)

(d) What must you add to T_n to obtain $T_{(n+1)}$? So what must you add to $2 \cdot T_n$ to obtain $2 \cdot T_{(n+1)}$? Now suppose your guess for T_n is correct. Use this and the connection between $2 \cdot T_n$ and $2 \cdot T_{(n+1)}$ to evaluate $2 \cdot T_{(n+1)}$.

(e) Explain why (d) does **not** imply that your guess of the value of $T_{(n+1)}$ is correct, but (d) does imply that **if** your guess for the value of T_n is correct **then** your guess for the value of $T_{(n+1)}$ is correct.

(f) In (a) you evaluated T_5. Use the conclusion of (d) (as stated in (e)) with $n = 5$ to verify that your guess for T_6 is correct.

(g) From (e) you know that your guess for T_6 is correct. Use the conclusion of (d) with $n = 6$ to verify that your guess for T_7 is correct.

(h) From (g) you know that your guess for T_7 is correct. Use the conclusion of (d) with $n = 7$ to verify that your guess for T_8 is correct.

(i) Explain how your computations in (a) and (d) allow you to conclude that, for each successive value of n, your formula for T_n is correct.

(j) Find a geometric argument that shows your formula for T_n is correct.

2.5. Consider the following diagram.

$$1$$

$$3 \quad 5$$

$$7 \quad 9 \quad 11$$

$$13 \quad 15 \quad 17 \quad 19$$

$$21 \quad 23 \quad 25 \quad 27 \quad 29$$

$$31 \quad 33 \quad 35 \quad 37 \quad 39 \quad 41$$

$$\vdots$$

So row 1 has the 1st odd natural number, row 2 has the next 2 odd natural numbers, row 3 has the next 3 odd natural numbers, and so on. We let S_n be the sum of the numbers in row n. We seek a formula for S_n.

(a) Compute the values of S_1, S_2, S_3, S_4 and S_5. Also, compute the values of $1^3 = 1 \cdot 1 \cdot 1$, $2^3 = 2 \cdot 2 \cdot 2$, $3^3 = 3 \cdot 3 \cdot 3$, $4^3 = 4 \cdot 4 \cdot 4$, and $5^3 = 5 \cdot 5 \cdot 5$.

(b) Explain why the 2nd triangular number tells you how many numbers are in the first 2 rows of the diagram. Explain why the 3rd triangular number tells you how many numbers are in the first 3 rows of the diagram. Explain why the 4th triangular number tells you how many numbers are in the first 4 rows of the diagram. Explain why the 5th triangular number tells you how many numbers are in the first 5 rows of the diagram. Explain why the nth triangular number tells you how many numbers are in the first n rows of the diagram. Explain why the $(n-1)$st triangular number tells you how many numbers are in the first $(n-1)$ rows of the diagram. Also, what must one add to $T_{(n-1)}$ to obtain T_n? Use this to write T_n in terms of $T_{(n-1)}$ and n.

(c) Determine the value of the sum of the numbers in the first 2 rows of the diagram. (You may want to use #2.1.) Determine the value of the sum of the numbers in the first 3 rows of the diagram. Determine the value of the sum of the numbers in the first 4 rows of the diagram. Determine the value of the sum of the numbers in the first 5 rows of the diagram. With n a natural number, determine the value of the sum of the numbers in the first n rows of the diagram. Determine the value of the sum of the numbers in the first $(n-1)$ rows of the diagram. Finally, use (b) to write the sum of the numbers in the first n rows of the diagram in terms of $T_{(n-1)}$ and n.

(d) Notice that S_3, the sum of the numbers in the 3rd row of the diagram, is equal to

$$S_3 = (\text{the sum of the numbers in the first 3 rows}) - (\text{the sum of the numbers in the first 2 rows}).$$

Similarly,

$$S_4 = (\text{the sum of the numbers in the first 4 rows}) - (\text{the sum of the numbers in the first 3 rows}),$$
$$S_5 = (\text{the sum of the numbers in the first 5 rows}) - (\text{the sum of the numbers in the first 4 rows}),$$

and so on. More generally,

$$S_n = (\text{the sum of the numbers in the first } n \text{ rows}) - (\text{the sum of the numbers in the first } (n-1) \text{ rows}).$$

Using this observation and (c), find a formula for S_n in terms of $T_{(n-1)}$ and n. Using #2.4, determine whether your formula for S_n agrees with the conjecture you made in (a); explain your reasoning. (You may want to use #1.7 (d) with $T_{(n-1)}$ in place of k.)

2.6. The first hexagonal number, H_1, is 1. The 2nd hexagonal number, H_2, is 6, which is the number of stars needed to outline a hexagon with each side comprised of 2 stars:

To find the 3rd hexagonal number H_3, we take the picture corresponding to the 2nd hexagonal number, and we embellish the picture with more stars so that we also have a hexagon with each side comprised of 3 stars; the upper 2 sides of the smaller hexagon lie

on the upper 2 sides of the larger hexagon. The total number of stars in the picture is the 3rd hexagonal number.

(a) The third hexagonal number H_3 is 15. Draw the picture described above that corresponds to H_3.

(b) To find the 4th hexagonal number H_4, we take the picture corresponding to the 3nd hexagonal number, and we embellish the picture with more stars so that we also have a hexagon with each side comprised of 4 stars; the upper 2 sides of the smaller hexagons lie on the upper 2 sides of the larger hexagon. The total number of stars in the picture is the 4th hexagonal number, H_4, which is equal to 28. Draw the picture described above that corresponds to H_4.

(c) To find the 5th hexagonal number H_5, we take the picture corresponding to the 4th hexagonal number, and we embellish the picture with more stars so that we also have a hexagon with each side comprised of 5 stars; the upper 2 sides of the smaller hexagons lie on the upper 2 sides of the larger hexagon. The total number of stars in the picture is the 5th hexagonal number, H_5. Draw the picture described above that corresponds to H_5. What is the value of H_5?

(d) To find the 6th hexagonal number H_6, we take the picture corresponding to the 5th hexagonal number, and we embellish the picture with more stars so that we also have a hexagon with each side comprised of 6 stars; the upper 2 sides of the smaller hexagons lie on the upper 2 sides of the larger hexagon. The total number of stars in the picture is the 6th hexagonal number, H_6. Draw the picture described above that corresponds to H_6. What is the value of H_6?

(e) Let n be a natural number. The picture corresponding to H_n is comprised of hexagons with sides of length 2, 3, 4,..., n; the upper 2 sides of the smaller hexagons lie on the upper 2 sides of the larger hexagon. Similarly, the picture corresponding to $H_{(n+1)}$ is comprised of hexagons with sides of length 2, 3, 4,..., $n, (n+1)$; the upper 2 sides of the smaller hexagons lie on the upper 2 sides of the larger hexagon. Suppose you have the picture corresponding to H_n. How many stars do you need to add to the picture to obtain the picture corresponding to $H_{(n+1)}$? Explain your reasoning.

(f) Compare the values of H_1, H_2, H_3, H_4, H_5 and H_6 to the values of the triangular numbers. Is there a correspondence? Can you guess the value of H_n? (You can check your guess for $n = 1$, $n = 2$, $n = 3$, $n = 4$, $n = 5$ and $n = 6$.) Can you guess the value of $H_{(n+1)}$? (You can check your guess for $n = 1$, $n = 2$, $n = 3$, $n = 4$ and $n = 5$.)

(g) Suppose your guess for the value of H_n in (f) is correct. Using (e) and your

supposition that you have correctly guessed the value of H_n, determine whether you have correctly guess the value of $H_{(n+1)}$.

(h) Explain why (g) does **not** imply that your guess of the value of $H_{(n+1)}$ is correct, but (g) does imply that **if** your guess for the value of H_n is correct **then** your guess for the value of $H_{(n+1)}$ is correct.

(i) In (d) you evaluated H_6. Use the conclusion of (g) (as stated in (h)) with $n = 6$ to verify that your guess for H_7 is correct.

(j) From (h) you know that your guess for H_7 is correct. Use the conclusion of (g) with $n = 7$ to verify that your guess for H_8 is correct.

(k) From (l) you know that your guess for H_8 is correct. Use (g) with $n = 8$ to verify that your guess for H_9 is correct.

(l) Explain how (f) and (g) allow you to conclude that, for each successive value of n, your formula for H_n is correct.

§3. Linear Combinations, Primes and Common Divisors.

Terminology: A linear combination of two natural numbers x and y is a sum or difference of multiples of x and y. For example, $6 \cdot 5 - 2 \cdot 7$ is a linear combination of 5 and 7.

3.1. (a) Make a list of the multiples of 7 between $1 \cdot 7$ and $7 \cdot 7$. Make a list of the multiples of 10 between $1 \cdot 10$ and $7 \cdot 10$. Find a pair of numbers, one from each of your lists, so that the difference between these numbers is 1. Using this, write 1 as a linear combination of 7 and 10.

(b) Write 2 as a linear combination of 7 and 10.

(c) Write 3 as a linear combination of 9 and 15.

(d) Write 6 as a linear combination of 9 and 15.

3.2 (a) Suppose m, n, x and y are natural numbers so that

$$m = 3 \cdot x + 5 \cdot y \qquad \text{and} \qquad n = 7 \cdot x - 10 \cdot y.$$

(So both m and n are linear combinations of x and y.) Demonstrate that $4 \cdot m - 2 \cdot n$ is also a linear combination of x and y. (So you need to demonstrate that $4 \cdot m - 2 \cdot n$ can be written in the form (some natural number)$\cdot x$+(some natural number)$\cdot y$.)

(b) Suppose m, n, x and y are natural numbers so that

$$m = 3 \cdot x + 5 \cdot y \qquad \text{and} \qquad n = 7 \cdot x - 10 \cdot y.$$

Let a and b represent natural numbers; demonstrate that $a \cdot m - b \cdot n$ is also a linear combination of x and y.

(c) Suppose m, n, x and y are natural numbers so that

$$m = r \cdot x + s \cdot y \qquad \text{and} \qquad n = 7 \cdot x - 10 \cdot y$$

where r and s are natural numbers. Demonstrate that $4 \cdot m - 2 \cdot n$ is also a linear combination of x and y.

(d) Suppose m, n, x and y are natural numbers so that

$$m = r \cdot x + s \cdot y \qquad \text{and} \qquad n = 7 \cdot x - 10 \cdot y$$

where r and s are natural numbers. Let a and b represent natural numbers; demonstrate that $a \cdot m - b \cdot n$ is also a linear combination of x and y.

(e) Suppose m, n, x and y are natural numbers so that

$$m = r \cdot x + s \cdot y \qquad \text{and} \qquad n = u \cdot x - v \cdot y$$

where r, s, u and v are natural numbers. Demonstrate that $4 \cdot m - 2 \cdot n$ is also a linear combination of x and y.

(d) Suppose m, n, x and y are natural numbers so that

$$m = r \cdot x + s \cdot y \qquad \text{and} \qquad n = u \cdot x - v \cdot y$$

where r, s, u and v are natural numbers. Let a and b represent natural numbers; demonstrate that $a \cdot m - b \cdot n$ is also a linear combination of x and y.

Terminology: Since each natural number n is equal to $1 \cdot n$, 1 is called a multiplicative identity. A natural number greater than 1 is called prime if it is divisible only by 1 and itself. (For example, 2, 3, 7 and 17 are prime; 15 and 9 are not.)

3.3. A natural number e is a multiplicative identity if, for every natural number n, $e \cdot n$ is equal to n. We want to show the natural numbers contain only one multiplicative identity.

(a) (Geometric approach) Suppose k is a natural number other than 1. So how small could k be? How do $k \cdot 5$ and 5 compare in size? Is it possible for $k \cdot 5$ to be equal to 5? Explain your reasoning.

(b) (Algebraic approach) Suppose e is a natural number, and suppose e is a multiplicative identity. Knowing how to multiply by 1, what is $e \cdot 1$? Using the assumption that e is a multiplicative identity, what is $e \cdot 1$? (Suggestion: Take n to be 1 in the sentence describing what it means for e to be a multiplicative identity.) Explain why this means e must equal 1.

(c) Using (a) or (b), explain why 1 is *the* multiplicative identity, not just *a* multiplicative identity. Explain why this means 1 is the *unique* multiplicative identity within the natural numbers.

3.4. (a) Briefly but clearly explain why 4, 6, 12 and 36 are **not** prime.

(b) Classify each natural number from 2 to 25 as prime or non-prime. Write each of these non-prime numbers as a product of primes. (For instance, $12 = 2 \cdot 2 \cdot 3$.) For the other non-primes between 2 and 25, it is possible to write each of these non-primes as a product of primes.

3.5. (a) Suppose you are given 17 pennies and you are asked to put them into stacks of 5. How many stacks will you have? How many pennies all together are in your stacks? How many (if any) pennies are left over?

(b) Find whole numbers q and r so that $17 = 5 \cdot q + r$, and r is smaller than 5. How do q and r relate to the number of stacks and the number of pennies left over?

(c) Suppose you are given 17 pennies and you are asked to put them into stacks of 5. How many stacks will you have? How many pennies all together are in your stacks? How many (if any) pennies are left over?

(d) Find whole numbers q and r so that $15 = 5 \cdot q + r$, and r is smaller than 5. How do q and r relate to the number of stacks and the number of pennies left over?

(e) Suppose you are given 17 pennies and you are asked to put them into stacks of 21. How many stacks will you have? How many pennies all together are in your stacks? How many (if any) pennies are left over?

(f) Find whole numbers q and r so that $17 = 21 \cdot q + r$, and r is smaller than 21. How do q and r relate to the number of stacks and the number of pennies left over?

(g) Suppose you are given n pennies (where n is a natural number). With these pennies, you create as many stacks of 5 pennies as possible. How many pennies can you have left over? (In particular, can you have 5 or more pennies left over?) Explain why there are whole numbers q and r so that $n = 5 \cdot q + r$. How do q and r relate to the number of stacks and the number of pennies left over?

(h) Suppose you are given n pennies (where n is a natural number). Suppose m is another natural number; imagine putting your n pennies into as many stack of m as possible. How many pennies can you have left over? (In particular, can you have m or more pennies left over?) Explain why there are whole numbers q and r so that $n = m \cdot q + r$. How do q and r relate to the number of stacks and the number of pennies left over? When will q equal 0? When will r equal 0?

3.6. **Recall:** Suppose we have natural numbers m and n with m smaller than n. Then either m divides n (so $n = m \cdot q$ for some natural number q), or $n = m \cdot q + r$ for some natural numbers q and r with r smaller than m. Thus for natural numbers m and n with m smaller than n, we have $n = m \cdot q + r$ where q is a natural number and r is a whole number smaller than m. (Recall that r is a whole number if either r is a natural number or r is zero.)

(a) We now consider the situation with n smaller than m. For instance, suppose $n = 10$ and $m = 35$. Find whole numbers q and r so that $n = m \cdot q + r$ with r smaller than m.

(b) Now suppose m and n are some natural numbers with n smaller than m. Find whole numbers q and r so that $n = m \cdot q + r$ with r smaller than m.

Recall: The numbers

$$0, 1, -1, 2, -2, 3, -3, 4, -4, 5, -5, \ldots$$

are called the integers.

(c) Say $n = -10$ and $m = 35$. Find an integer s and a whole number t so that $n = m \cdot s + t$ with t smaller than m. (Suggestion: Try $s = -1$.)

(d) Now suppose m and n are natural numbers with n smaller than m. Find an integer s and a whole number t so that $-n = m \cdot s + t$ with t smaller than m. (Suggestion: Try $s = -1$.)

(e) Now suppose $n = 37$ and $m = 11$. First find a natural number q and a whole number r so that $n = m \cdot q + r$ with r smaller than m. Now find an integer s and a whole number t so that $-n = m \cdot s + t$ with t smaller than m. (Suggestion: Multiply both sides of your equation $n = m \cdot q + r$ by -1. Then try $s = -q - 1$.)

(f) Now suppose m and n are natural numbers with m smaller than n. So we know there is a natural number q and a whole number r so that $n = m \cdot q + r$ with r smaller than m. Now find an integer s and a whole number t so that $-n = m \cdot s + t$ with t smaller than m. (Suggestion: Multiply both sides of your equation $n = m \cdot q + r$ by -1. Then try $s = -q - 1$.)

Terminology: We say a natural number d is a divisor of another natural number n if n is divisible by d, i.e. $n = d \cdot k$ for some natural number k. We say d is a common divisor of m and n if d is both a divisor of m and of n. We say a common divisor d of m and n is the greatest common divisor if d is larger than every other common divisor of m and n.

3.7. (a) Find the common divisors of 9 and 15. Which is the greatest common divisor?

(b) Find the common divisors of 60 and 84. Which is the greatest common divisor? Find the common divisors of 9 and 17. Which is the greatest common divisor?

(c) Let m and n represent natural numbers. Explain why m and n have at least one common divisor, and why m and n have a greatest common divisor. (What natural number divides every other natural number? How do diviors of a number compare in size to that number? So how many divisors can a number have, infinitely many or only finitely many?)

(d) Say n is a natural number and 12 divides n List the common divisors of 12 and n; identify the greatest common divisor.

(e) Say m and n are natural numbers and m divides n. Describe the common divisors of m and n. What is the greatest common divisor of m and n?

(f) Say n and q are natural numbers so that $n = 12 \cdot q + 3$. Explain why 3 is a common divisor of n and 12. If d is a divisor of n and 12, why must d divide 3? (Suggestion: Write 3 in terms of n and 12.) Explain why 3 is the greatest common divisor of n and 12.

(g) Say n and q are natural numbers so that $n = 12 \cdot q + 9$. Explain why any common divisor of n and 12 is also a divisor of 9. List the common divisors of n and 12; identify the greatest common divisor.

(h) Say m, n and q are natural numbers so that $n = m \cdot q + 9$. Explain why any common divisor of n and m is also a divisor of 9. Explain why any common divisor of m and 9 is also a divisor of n. Explain why the greatest common divisor of m and 9 is also the greatest common divisor of m and n.

(i) Say m, n, q and r are natural numbers so that $n = m \cdot q + r$. Explain why any common divisor of n and m is also a divisor of r. Explain why any common divisor of m and r is also a divisor of n. Explain why the greatest common divisor of m and r is also the greatest common divisor of m and n. (How does the list of common divisors of m and r compare to the list of common divisors of m and n?)

3.8. **Recall:** In #3.7 we saw that when we have natural numbers n, m and q with $n = m \cdot q$, then the greatest common divisor of m and n is m. When we have natural numbers n and m, and whole numbers q and r, with $n = m \cdot q + r$, then the greatest common divisor of n and m is equal to the greatest common divisor of m and r.

(a) Take $n_1 = 24$ and $m_1 = 9$. What is the greatest common divisor of n_1 and m_1? Find whole numbers q_1 and r_1 so that $n_1 = m_1 \cdot q_1 + r_1$ with r_1 smaller than m_1.

(b) Now take $n_2 = m_1 = 9$ and $m_2 = r_1$. Find whole numbers q_2 and r_2 so that $n_2 = m_2 \cdot q_2 + r_2$ with r_2 smaller than m_2.

(c) Now take $n_3 = m_2$ and $m_3 = r_2$. Find whole numbers q_3 and r_3 so that $n_3 = m_3 \cdot q_3 + r_3$ with r_3 smaller than m_3.

(d) Use (b) to write r_2 as a linear combination of n_2 and m_2. Remembering that $n_2 = m_1$ and $m_2 = r_1$, briefly explain why this means you have written r_2 as a linear combination of m_1 and r_1.

(e) Use (a) to write r_1 as a linear combination of n_1 and m_1. Now substitute this expression for r_1 into your formula for r_2 found in (d).

(f) Using (e), demonstrate that r_2 is a linear combination of n_1 and m_1.

Abbreviation: "gcd" stands for "greatest common divisor."

3.9. Suppose n_1 and m_1 are natural numbers. Then we know from #3.4 that we can find whole numbers q_1 and r_1 so that r_1 is smaller than m_1 and

$$n_1 = m_1 \cdot q_1 + r_1 \qquad \text{(Equation 1)}.$$

Here r_1 is called the "remainder term" in Equation 1. Provided r_1 is not 0, we construct Equation 2 from Equation 1 as follows: Set $n_2 = m_1$ and $m_2 = r_1$. Find whole numbers q_2 and r_2 so that r_2 is smaller than m_2 and

$$n_2 = m_2 \cdot q_2 + r_2 \qquad \text{(Equation 2)}.$$

Here r_2 is called the remainder term of Equation 2. Provided r_2 is not 0, we construct Equation 3 from Equation 2 as follows: Set $n_3 = m_2$ and $m_3 = r_2$. Find whole numbers q_3 and r_3 so that r_3 is smaller than m_3 and

$$n_3 = m_3 \cdot q_3 + r_3 \qquad \text{(Equation 3)}.$$

Here r_3 is called the remainder term of Equation 3. In a similar manner, if r_3 is not 0 we construct Equation 4 from Equation 3, and if r_4 is not 0 we construct Equation 5 from Equation 4, and so on. So eventually we have many equations:

$$\begin{aligned}
n_1 &= m_1 \cdot q_1 + r_1 && \text{with } r_1 \text{ smaller than } m_1;\\
n_2 &= m_1, \quad \text{and} \quad m_2 = r_1, && \text{and}\\
n_2 &= m_2 \cdot q_2 + r_2 && \text{with } r_2 \text{ smaller than } m_2;\\
n_3 &= m_2, \quad \text{and} \quad m_3 = r_2, && \text{and}\\
n_3 &= m_3 \cdot q_3 + r_3 && \text{with } r_3 \text{ smaller than } m_3;\\
n_4 &= m_3, \quad \text{and} \quad m_4 = r_3, && \text{and}\\
n_4 &= m_4 \cdot q_4 + r_4 && \text{with } r_4 \text{ smaller than } m_4;\\
&\vdots\\
n_k &= m_{(k-1)}, \quad \text{and} \quad m_k = r_{(k-1)}, && \text{and}\\
n_k &= m_k \cdot q_k + r_k && \text{with } r_k \text{ smaller than } m_k;\\
n_{(k+1)} &= m_k, \quad \text{and} \quad m_{(k+1)} = r_k, && \text{and}\\
n_{(k+1)} &= m_{(k+1)} \cdot q_{(k+1)} + r_{(k+1)} && \text{with } r_{(k+1)} \text{ smaller than } m_{(k+1)}.
\end{aligned}$$

(a) Explain why the second remainder term r_2 is smaller than the first remainder term r_1.

(b) Explain why the third remainder term r_3 is smaller than the second remainder term r_2.

(c) Explain why the fourth remainder term r_4 is smaller than the third remainder term r_3.

(d) Explain why the fifth remainder term r_5 is smaller than the fourth remainder term r_4.

(e) Suppose we know that the kth remainder term r_k is smaller than the $(k+1)$st remainder term $r_{(k-1)}$. Explain why $r_{(k+1)}$ must be smaller than r_k.

(f) Explain why, as we continue this construction, the remainder term in some equation must be 0.

3.10. Suppose n_1 and m_1 are natural numbers, and we build equations as we did in #3.9. So we have:

$$\begin{aligned}
n_1 &= m_1 \cdot q_1 + r_1 \qquad \text{with } r_1 \text{ smaller than } m_1;\\
n_2 &= m_1, \quad \text{and} \quad m_2 = r_1, \qquad \text{and}\\
n_2 &= m_2 \cdot q_2 + r_2 \qquad \text{with } r_2 \text{ smaller than } m_2;\\
n_3 &= m_2, \quad \text{and} \quad m_3 = r_2, \qquad \text{and}\\
n_3 &= m_3 \cdot q_3 + r_3 \qquad \text{with } r_3 \text{ smaller than } m_3;\\
n_4 &= m_3, \quad \text{and} \quad m_4 = r_3, \qquad \text{and}\\
n_4 &= m_4 \cdot q_4 + r_4 \qquad \text{with } r_4 \text{ smaller than } m_4;\\
&\vdots\\
n_k &= m_{(k-1)}, \quad \text{and} \quad m_k = r_{(k-1)}, \qquad \text{and}\\
n_k &= m_k \cdot q_k + r_k \qquad \text{with } r_k \text{ smaller than } m_k;\\
n_{(k+1)} &= m_k, \quad \text{and} \quad m_{(k+1)} = r_k, \qquad \text{and}\\
n_{(k+1)} &= m_{(k+1)} \cdot q_{(k+1)} + r_{(k+1)} \qquad \text{with } r_{(k+1)} \text{ smaller than } m_{(k+1)}.
\end{aligned}$$

(a) Suppose r_1 is not 0. (So m_2 is not 0.) Using your result from #3.7, explain why the gcd of n_1 and m_1 is equal to the gcd of m_1 and r_1. Also, explain why the gcd of n_2 and m_2 is equal to the gcd of m_2 and r_2. Using this, explain why the gcd of m_2 and r_2 is equal to the gcd of m_1 and r_1. Finally, recalling the way in which n_2 and m_2 were defined, explain why the gcd of m_2 and r_2 is equal to the gcd of n_1 and m_1.

(b) Suppose r_1 is not 0, but r_2 is 0; explain why this means the gcd of m_2 and r_2 is m_2, and conclude that the gcd of n_1 and m_1 is m_2.

(c) Suppose r_1 and r_2 are not 0. (So m_3 is not 0.) Remembering the way in which n_3 and m_3 were defined, explain why the gcd of m_3 and r_3 is equal to the gcd of m_2 and r_2. Then using (a), conclude that the gcd of m_3 and r_3 is equal to the gcd of n_1 and m_1.

(d) Suppose r_1 and r_2 are not 0, but that r_3 is 0; explain why this means the gcd of m_3 and r_3 is m_3, and conclude that the gcd of n_1 and m_1 is m_3.

(e) Suppose r_1, r_2 and r_3 are not 0. (So m_3 and m_4 are not 0.) Explain why the gcd of m_4 and r_4 is equal to the gcd of m_3 and r_3. Then using (c), conclude that the gcd of m_4 and r_4 is equal to the gcd of n_1 and m_1.

(f) Suppose r_1, r_2 and r_3 are not 0, but that r_4 is 0; explain why this means the gcd of m_4 and r_4 is m_4, and conclude that the gcd of n_1 and m_1 is m_4.

(g) Suppose r_1, r_2, r_3 and r_4 are not 0. (So m_5 is not 0.) Explain why the gcd of m_5 and r_5 is equal to the gcd of m_4 and r_4. Then using (e), conclude that the gcd of m_5 and r_5 is equal to the gcd of n_1 and m_1.

(h) Suppose r_1, r_2, r_3 and r_4 are not 0, but that r_5 is 0; conclude that the gcd of n_1 and m_1 is m_5.

(i) Suppose $r_1, r_2, r_3, r_4, \ldots, r_k$ are not 0. (So $m_{(k+1)}$ is not 0.) Explain why the gcd of $m_{(k+1)}$ and $r_{(k+1)}$ is equal to the gcd of n_1 and m_1.

(j) Suppose $r_1, r_2, r_3, r_4, \ldots, r_k$ are not 0, but that $r_{(k+1)}$ is 0; conclude that the gcd of n_1 and m_1 is $m_{(k+1)}$.

3.11. Suppose n_1 and m_1 are natural numbers, and we build equations as we did in #3.9. So we have:

$$
\begin{aligned}
n_1 &= m_1 \cdot q_1 + r_1 && \text{with } r_1 \text{ smaller than } m_1;\\
n_2 &= m_1, \quad \text{and} \quad m_2 = r_1, && \text{and}\\
n_2 &= m_2 \cdot q_2 + r_2 && \text{with } r_2 \text{ smaller than } m_2;\\
n_3 &= m_2, \quad \text{and} \quad m_3 = r_2, && \text{and}\\
n_3 &= m_3 \cdot q_3 + r_3 && \text{with } r_3 \text{ smaller than } m_3;\\
n_4 &= m_3, \quad \text{and} \quad m_4 = r_3, && \text{and}\\
n_4 &= m_4 \cdot q_4 + r_4 && \text{with } r_4 \text{ smaller than } m_4;\\
&\vdots\\
n_k &= m_{(k-1)}, \quad \text{and} \quad m_k = r_{(k-1)}, && \text{and}\\
n_k &= m_k \cdot q_k + r_k && \text{with } r_k \text{ smaller than } m_k;\\
n_{(k+1)} &= m_k, \quad \text{and} \quad m_{(k+1)} = r_k, && \text{and}\\
n_{(k+1)} &= m_{(k+1)} \cdot q_{(k+1)} + r_{(k+1)} && \text{with } r_{(k+1)} \text{ smaller than } m_{(k+1)}.
\end{aligned}
$$

(a) Demonstrate that r_1 is a linear combination of n_1 and m_1, and r_2 is a linear combination of n_2 and m_2. Then, remembering how n_2 and m_2 are defined,

explain why r_2 is a linear combination of n_1 and m_1. (You may want to use the result of #3.2.)

(b) Write r_3 as a linear combination of n_3 and m_3. Then, remembering how n_3 and m_3 are defined, explain why r_3 is a linear combination of r_1 and r_2. Now use your result from (a) and #3.2 to explain why r_3 is a linear combination of n_1 and m_1.

(c) Following the method used in (b), explain why r_4 is a linear combination of n_1 and m_1.

(d) Using your above results, explain why r_5 is a linear combination of n_1 and m_1.

(e) Suppose we know that $r_{(k-1)}$ and r_k are linear combinations of n_1 and m_1. Explain why $r_{(k+1)}$ is also a linear combination of n_1 and m_1.

(f) With $k = 5$, explain why we already know that $r_{(k-1)}$ and r_k are linear combinations of n_1 and m_1. What does (e) then tell us about r_6?

(g) With $k = 6$, explain why we already know that $r_{(k-1)}$ and r_k are linear combinations of n_1 and m_1. What does (e) then tell us about r_7?

(h) With $k = 7$, explain why we already know that $r_{(k-1)}$ and r_k are linear combinations of n_1 and m_1. What does (e) then tell us about r_8?

(i) Suppose we've constructed (at least) 25 equations. Can (e) be used to deduce that r_{25} is a linear combination of n_1 and m_1? Clearly explain your reasoning.

(j) Suppose we've constructed (at least) 100 equations. Can (e) be used to deduce that r_{100} is a linear combination of n_1 and m_1? Clearly explain your reasoning.

(k) Suppose we've constructed (at least) 1000 equations. Can (e) be used to deduce that r_{1000} is a linear combination of n_1 and m_1? Clearly explain your reasoning.

3.12. Suppose n_1 and m_1 are natural numbers, and we construct equations as in #3.10. By #3.10, we know that eventually the remainder term in one of these equations will be 0. Thus for some natural number k (being the number of equations constructed

before the remainder term is 0), we have:

$$\begin{aligned}
n_1 &= m_1 \cdot q_1 + r_1 \qquad \text{with } r_1 \text{ smaller than } m_1;\\
n_2 &= m_1, \quad \text{and} \quad m_2 = r_1, \qquad \text{and}\\
n_2 &= m_2 \cdot q_2 + r_2 \qquad \text{with } r_2 \text{ smaller than } m_2;\\
n_3 &= m_2, \quad \text{and} \quad m_3 = r_2, \qquad \text{and}\\
n_3 &= m_3 \cdot q_3 + r_3 \qquad \text{with } r_3 \text{ smaller than } m_3;\\
n_4 &= m_3, \quad \text{and} \quad m_4 = r_3, \qquad \text{and}\\
n_4 &= m_4 \cdot q_4 + r_4 \qquad \text{with } r_4 \text{ smaller than } m_4;\\
&\vdots\\
n_k &= m_{(k-1)}, \quad \text{and} \quad m_k = r_{(k-1)}, \qquad \text{and}\\
n_k &= m_k \cdot q_k + r_k \qquad \text{with } r_k \text{ smaller than } m_k;\\
n_{(k+1)} &= m_k, \quad \text{and} \quad m_{(k+1)} = r_k, \qquad \text{and}\\
n_{(k+1)} &= m_{(k+1)} \cdot q_{(k+1)}.
\end{aligned}$$

Using your conclusions from #3.10 and #3.11, explain why the gcd of n_1 and m_1 is a linear combination of n_1 and m_1. (This result is called the Euclidean algorithm.)

3.13. (a) Say b is a natural number. Suppose 7 divides $10 \cdot b$. As in #3.2 (a), write 1 as a linear combination of 7 and 10. (So you have an equation: 1= some linear combination of 7 and 10.) Then multiply both sides of the equation by b. Using this new equation and your assumptions, explain why 7 must divide b. (You may want to use the result of #1.9.)

(b) Say a and b are natural numbers and 7 does not divide a, but 7 does divide $a \cdot b$. Using #3.12 with $n_1 = 7$ and $m_1 = a$, explain why 1 can be written as a linear combination of 7 and a. Then use the techniques of (a) to explain why b must be divisible by 7.

(c) Say a and b are natural numbers and p is a prime. Suppose p does not divide a, but p does divide $a \cdot b$. Explain why 1 can be written as a linear combination of p and a (again, you may want to use your result from #3.12). Then explain why b must be divisible by p.

(d) Let m and n be natural numbers, and p a prime. Say p divides $m \cdot n$; explain why either p divides m or p divides n (or both). (Certainly either p divides m or p does not divide m. If p divides m then we are done. If p does not divide m, what does (c) tell you?)

3.14. (a) Suppose that x and y are integers so that $x \cdot y = 12$. Is it necessarily the case that either 6 divides x or 6 divides y? Either deduce that this is the case, or present a specific example to show this is not the case.

(b) Suppose 6 divides $x \cdot y$ where x and y are integers. Does this mean that either 6 divides x or 6 divides y? Either deduce that this is the case, or present a specific example to show this is not the case.

(c) Suppose 9 divides $x \cdot y$ where x and y are integers. Does this mean that either 9 divides x or 9 divides y? Either deduce that this is the case, or present a specific example to show this is not the case.

(d) Suppose p is a prime and $2 \cdot p$ divides $x \cdot y$ where x and y are integers. Does this mean that either $2 \cdot p$ divides x or $2 \cdot p$ divides y? Either deduce that this is the case, or present a specific example to show this is not the case.

(e) Suppose p and q are primes, and $p \cdot q$ divides $x \cdot y$ where x and y are integers. Does this mean that either $p \cdot q$ divides x or $p \cdot q$ divides y? Either deduce that this is the case, or present a specific example to show this is not the case.

(f) Suppose n is a natural number that is not prime. Suppose also that n divides $x \cdot y$ where x and y are integers. Does this mean that either n divides x or n divides y? Either deduce that this is the case, or present a specific example to show this is not the case.

3.15. (a) For each natural number between 2 and 25, classify the number as prime, or write the number as a product of primes.

(b) Can $12 \cdot 5$ be written as a product of primes? Briefly but clearly explain your answer.

(c) Can $12 \cdot 7$ be written as a product of primes? Briefly but clearly explain your answer.

(d) Suppose n is a natural number, and $n = 12 \cdot p$ where p is a prime. Can n be written as a product of primes? Briefly but clearly explain your answer.

(e) Suppose n is a natural number, and $n = 18 \cdot p$ where p is a prime. Can n be written as a product of primes? Briefly but clearly explain your answer.

(f) Suppose n is a natural number with $n = m \cdot k$ where m and k are natural numbers between 2 and 25. Can n be written as a product of primes? Briefly but clearly explain your answer. (You may want to use your previous conclusions, especially from (a).)

(g) Say n is a natural number greater than 1, and suppose we already know that each natural number smaller than n can be written as a product of primes. Can n be

written as a product of primes? Present a clear and compelling argument. (**Note:** If n is prime, then there is nothing to do. So if n is **not** prime, can n be written as a product of natural numbers smaller than n? What are we assuming here about numbers smaller than n? What can you then conclude about a product of natural numbers smaller than n?)

(h) Explain why (g) does **not** imply that we necessarily know that each natural number smaller than n can be written as a product of primes. Explain why (g) does imply that **if** each natural number smaller than n can be written as a product of primes, **then** n can be written as a product of primes.

(i) By (a), we know that each natural number between 2 and 25 can be written as a product of primes. Use (g) with $n = 26$ to deduce that 26 can be written as a product of primes.

(j) By (i), we know that 26 can be written as a product of primes. Use (g) with $n = 27$ to deduce that 27 can be written as a product of primes.

(k) By (j), we know that 27 can be written as a product of primes. Use (g) with $n = 28$ to deduce that 28 can be written as a product of primes.

(l) By (k), we know that 28 can be written as a product of primes. Use (g) with $n = 29$ to deduce that 29 can be written as a product of primes.

(m) Can (g) be used to show that 291 can be written as a product of primes? Can (g) be used to show that 6325 can be written as a product of primes? Clearly explain your reasoning.

3.16. **Recall:** Suppose p is a prime and a, b are natural numbers. If p divides $a \cdot b$ but p does **not** divide a, then p must divide b.

Verifiable fact: 61 is a prime.

(a) Suppose p is a prime that divides 183. (Notice that $183 = 3 \cdot 61$.) Explain why either p divides 3 or p divides 61. Then, remembering that 3 and 61 are prime, explain why either $p = 3$ or $p = 61$. (What are the divisors of 3 and 61?)

(b) Explain why (a) implies that the only primes that divide 183 are 3 and 61. (We already know that 3 and 61 divide 183. You need to explain why no other prime can possibly divide 183.)

3.17. We show here that a prime cannot be written as a product of primes in exactly one way.

(a) The number 2 is itself prime, so certainly we can write 2 as a "product" of one prime. Explain why there is no other way to write 2 as a product of primes. (Which numbers divide 2? Which of these divisors are prime?)

(b) Explain why there is only one way to write 3 as a product of primes.

(c) Suppose p is prime. Explain why no prime other than p divides p. Then explain why the only way to write p as a product of primes is simply to write p as p, a product of one prime.

3.18. In #3.15 we saw that each natural number can be written as a product of primes. We want to deduce that there is esentially only one way to write a natural number as a product of primes. (Since 1 is not divisible by any primes, we consider 1 to be an "empty product" of primes.) As seen in #3.17, each prime can be written in exactly one way as a product of primes. Suppose we have a non-prime natural number n that is larger than 3. To factor n into a product of primes, we can begin with a prime p that divides n. Then we can write n as $p \cdot k$ for some natural number k. Then we continue to factor k as a product of primes.

(a) Find a natural number m so that $105 = 3 \cdot m$. Now write m as a product of primes; tThis allows you to write 105 as a product of primes. Next, find a natural number k so that $105 = 5 \cdot k$. Now write k as a product of primes; again, this allows you to write 105 as a product of primes. Does this give you two truely different ways of writing 105 as a product of primes? In what sense are these factorizations of 105 essentially the same?

For (b)–(j), suppose n is a natural number larger than 3. Suppose also that each natural number smaller than n can be written in essentially one way as a product of primes. If n is prime, then we already know n can be written in only one way as a product of primes; so suppose n is not prime. Let p and q be two primes that divide n.

(b) Expalin why this means $n = p \cdot k$ for some natural number k, and $n = q \cdot m$ for some natural number m. Also, explain why k and m are necessarily smaller than n.

(c) Let k and m be as in (b). Explain why either p divides q or p divides m. (Does p divide n? How does n relate to q and m?)

(d) Suppose p divides q. Explain why this means $p = q$. (What primes divide q? Remember the assumptions on q.) Still supposing p divides q, explain why this means $p \cdot k - p \cdot m = 0$; then deduce that $k - m = 0$ and hence $k = m$. (You may want to use #1.12.) Finally, using our assumption regarding numbers smaller than n, explain why our initial factorizations of n as $p \cdot k$ and as $q \cdot m$ lead to essentially the same factorization of n as a product of primes.

(e) Suppose p does not divide q. Explain why this means p is not equal to q. (What primes divide q? Remember your assumptions on p and q. You may want to

use #3.17.) Then using the conclusion that p does not equal q, explain why this means q does not divide p.

(f) Again suppose p does not divide q. Explain why this means p must divide m. Then explain why this means $m = p \cdot s$ for some natural number s. Explain why s is necessarily smaller than m, and so s is necessarily smaller than n.

(g) Still suppose p does not divide q. Explain why this means q must divide k. Then explain why this means $k = q \cdot t$ for some natural number t. Explain why t is necessarily smaller than k, and so t is necessarily smaller than n.

(h) Still suppose p does not divide q. Using (f) and (g), explain why $n = p \cdot q \cdot t$ and $n = q \cdot p \cdot s$ where s and t are as in (f) and (g). From this deduct that $p \cdot q \cdot (t - s) = 0$; then deduce that $t - s = 0$ and hence $t = s$.

(i) Still suppose p does not divide q. Given the suppositions and your conclusions in (h), can there be essentially differenct ways to factor t and s as products of primes? Explain your reasoning. (Remember what we are assuming about numbers smaller than n.)

(j) Still suppose p does not divide q. Using (h) and (i), explain why our factorizations of n as $p \cdot k$ and as $q \cdot m$ lead to essentially the same factorization of n as a product of primes.

(k) Explain why (d) and (j) allow us to conclude that if each natural number smaller than n can be factored in essentially one way as a product of primes, then n can be factored in essentially one way as a product of primes.

(l) We know from #3.17 that each natural number smaller than 4 can be factored in essentially one way as a product of primes. Use (k) to conclude that 4 can factored in essentially one way as a product of primes.

(m) We know from (l) that each natural number smaller than 5 can be factored in essentially one way as a product of primes. Use (k) to conclude that 5 can factored in essentially one way as a product of primes.

(n) We know from (m) that each natural number smaller than 6 can be factored in essentially one way as a product of primes. Use (k) to conclude that 6 can factored in essentially one way as a product of primes.

(o) We know from (n) and #3.17 that each natural number smaller than 8 can be factored in essentially one way as a product of primes. Use (k) to conclude that 8 can factored in essentially one way as a product of primes.

(p) We know from (o) that each natural number smaller than 9 can be factored in essentially one way as a product of primes. Use (k) to conclude that 9 can factored in essentially one way as a product of primes.

(q) Can (k) and #3.17 be used to show that 25 can factored in essentially one way as a product of primes? Can (k) and #3.17 be used to show that 40 can factored in essentially one way as a product of primes? Can (k) and #3.17 be used to show that 100 can factored in essentially one way as a product of primes? Can (k) and #3.17 be used to show that any natural number n can factored in essentially one way as a product of primes? Clearly explain your reasoning.

3.19. We want to deduce that there are infinitely many primes. (So do not already assume this!) Say we have a list of finitely many primes: $2, 3, 5, 7, \ldots, p$. Let n be the product of the primes in this list; so $n = 2 \cdot 3 \cdot 5 \cdot 7 \cdot \ldots \cdot p$.

(a) Briefly explain why $n+1$ can be written as a product of primes. (Is $n+1$ a natural number? What do you know about natural numbers and products of primes?)

(b) Suppose n and $n + 1$ are divisible by d, where d represents a natural number. Deduce that d must be 1. (You may want to use your result from #5(d).)

(c) Clearly explain why $n + 1$ is not divisible by any of the primes in the list $2, 3, 5, 7, \ldots, p$. (Use part (b)!)

(d) Clearly explain why there is another prime besides those in the list $2, 3, 5, 7, \ldots, p$.

(e) Clearly explain why this means there cannot be only finitely many primes.

§4. Congruences.

Notation: Given integers a, b, the notation $a \equiv b \pmod 7$ means that 7 divides $a - b$. For instance, $3 \equiv 10 \pmod 7$ and $-12 \equiv 5 \pmod 7$. More generally, given a natural number m and integers a, b, the notation $a \equiv b \pmod m$ means that m divides $a - b$. (The symbol $\equiv$ is shorthand for "is congruent to", and "mod" is shorthand for "modulo".)

4.1. We want to establish that congruence modulo a fixed natural number m is "reflexive;" that is, for an integer x, $x \equiv x \pmod m$.

(a) Using the definition of congruence, explain why $3 \equiv 3 \pmod{10}$.

(b) Using the definition of congruence, explain why $5 \equiv 5 \pmod{12}$.

(c) Let m be a natural number. Using the definition of congruence, explain why $3 \equiv 3 \pmod m$.

(d) Let m be a natural number. Using the definition of congruence, explain why $x \equiv x \pmod m$ for any integer x.

4.2. We want to establish that congruence modulo a fixed natural number m is "symmetric;" that is, for integers x and y, $x \equiv y \pmod m$ exactly when $y \equiv x \pmod m$.

(a) Explain why $17 \equiv 11 \pmod 6$; then explain why $11 \equiv 17 \pmod 6$.

(b) Suppose k is an integer so that $17 \equiv k \pmod 6$. Deduce that $k \equiv 17 \pmod 6$.

(c) Suppose k and n are integers so that $k \equiv n \pmod 6$. Deduce that $n \equiv k \pmod 6$.

(d) Suppose m is a natural number, and k and n are integers so that $k \equiv n \pmod m$. Deduce that $n \equiv k \pmod m$.

(e) Suppose m is a natural number and x and y are integers. Using (d), explain why $x \equiv y \pmod m$ exactly when $y \equiv x \pmod m$. (So you must explain two things: You must show that if $x \equiv y \pmod m$ then $y \equiv x \pmod m$; you also must show that if $y \equiv x \pmod m$ then $x \equiv y \pmod m$.)

4.3. We want to establish that congruences modulo a fixed natural number m are "transitive;" that is, if k, ℓ and n are integers with $k \equiv \ell \pmod m$ and $\ell \equiv n \pmod m$ then $k \equiv n \pmod m$.

(a) Suppose n is an integer so that $11 \equiv k \pmod 6$. Using the definition of congruence and the fact that $17 \equiv 11 \pmod 6$, explain why $17 \equiv k \pmod 6$. (Notice that $17 - k = (17 - 11) + (11 - k)$. What do you already know about $17 - 11$ and $11 - k$?)

(b) Suppose ℓ and n are integers so that $17 \equiv \ell \pmod 6$ and $\ell \equiv n \pmod 6$. Using the definition of congruence, explain why $17 \equiv n \pmod 6$.

(c) Suppose k, ℓ and n are integers so that $k \equiv \ell \pmod 6$ and $\ell \equiv n \pmod 6$. Using the definition of congruence, explain why $k \equiv n \pmod 6$.

(d) Suppose m is a natural number and k, ℓ and n are integers so that $k \equiv \ell \pmod{m}$ and $\ell \equiv n \pmod{m}$. Using the definition of congruence, explain why $k \equiv n \pmod{m}$.

Terminology Since congruence modulo m is reflexive, symmetric and transitive, congruence modulo m is called an equivalence relation.

4.4. (a) Suppose k, n are integers so that $k \equiv n \pmod{7}$. (So $k - n$ is divisible by 7; equivalently, 7 divides $k - n$.) Deduce that $k + 3 \equiv n + 3 \pmod{7}$ and that $k - 5 \equiv n - 5 \pmod{7}$. (So you must deduce that $(k+3) - (n+3)$ is divisible by 7, and that $(k - 5) - (n - 5)$ is divisible by 7.)

(b) Suppose k, n are integers so that $k \equiv n \pmod{7}$. Let x denote another integer. Deduce that $k + x \equiv n + x \pmod{7}$ and that $k - x \equiv n - x \pmod{7}$.

(c) Suppose m is a natural number, and suppose k, n are integers so that $k \equiv n \pmod{m}$. Deduce that $k+3 \equiv n+3 \pmod{m}$ and that $k-5 \equiv n-5 \pmod{m}$.

(d) Suppose m is a natural number, and suppose k, n are integers so that $k \equiv n \pmod{m}$. Let x denote another integer. Deduce that $k + x \equiv n + x \pmod{m}$ and that $k - x \equiv n - x \pmod{m}$.

(e) Suppose k, n are integers so that $k \equiv n \pmod{7}$. Suppose also that x and y are integers so that $x \equiv y \pmod{7}$. Deduce that $k + x \equiv n + y \pmod{7}$ and that $k - x \equiv n - y \pmod{7}$. (Notice that $(k + x) - (n + y) = (k - n) + (x - y)$. What are we assuming about $k - n$ and $x - y$?)

(f) Suppose m is a natural number, and suppose k, n are integers so that $k \equiv n \pmod{m}$. Suppose also that x and y are integers so that $x \equiv y \pmod{m}$. Deduce that $k + x \equiv n + y \pmod{m}$ and that $k - x \equiv n - y \pmod{m}$.

(g) Suppose k and n are integers with $k \equiv n \pmod{7}$. Explain why $3 \cdot k \equiv 3 \cdot n \pmod{7}$ and $k \cdot 3 \equiv n \cdot 3 \pmod{7}$.

(h) Suppose x, k and n are integers with $k \equiv n \pmod{7}$. Explain why $x \cdot k \equiv x \cdot n \pmod{7}$ and $k \cdot x \equiv n \cdot x \pmod{7}$.

(i) Suppose m is a natural number and k and n are integers with $k \equiv n \pmod{m}$. Explain why $3 \cdot k \equiv 3 \cdot n \pmod{m}$ and $k \cdot 3 \equiv n \cdot 3 \pmod{m}$.

(j) Suppose m is a natural number and k and n are integers with $k \equiv n \pmod{m}$. Let x be an integer. Explain why $x \cdot k \equiv x \cdot n \pmod{m}$ and $k \cdot x \equiv n \cdot x \pmod{m}$.

(k) Suppose k and n are integers with $k \equiv n \pmod{7}$. Suppose also that x and y are integers with $x \equiv y \pmod{7}$. Explain why $x \cdot k \equiv y \cdot n \pmod{7}$. (Notice that $x \cdot k - y \cdot n = (x \cdot k - x \cdot n) + (x \cdot n - y \cdot n)$. What do our assumptions and (i) tell us about $(x \cdot k - x \cdot n)$ and $(x \cdot n - y \cdot n)$?)

(l) Suppose m is a natural number and k and n are integers with $k \equiv n \pmod{m}$. Suppose also that x and y are integers with $x \equiv y \pmod{7}$. Explain why $x \cdot k \equiv y \cdot n \pmod{m}$.

Notation: We write n^2 to denote $n \cdot n$, n^3 to denote $n \cdot n \cdot n$, n^4 to denote $n \cdot n \cdot n \cdot n$, etc.

4.5. (a) Suppose n and a are integers with $n \equiv a \pmod{7}$. Deduce that

$$n^2 \equiv n \cdot a \pmod{7} \qquad \text{and} \qquad n \cdot a \equiv a^2 \pmod{7}.$$

Then deduce that $n^2 \equiv a^2 \pmod{7}$. (You may want to use #4.4.)

(b) Suppose n and a are integers with $n^2 \equiv a^2 \pmod{7}$. Use this to deduce that

$$n^3 \equiv n \cdot a^2 \pmod{7}.$$

Explain why $a^2 \equiv a^2 \pmod{7}$, then deduce that

$$n \cdot a^2 \equiv a^3 \pmod{7}.$$

Then deduce that

$$n^3 \equiv a^3 \pmod{7}.$$

(c) Suppose that n, a and k are natural numbers. Suppose also that $n^k \equiv a^k \pmod{7}$. Deduce that

$$n^{k+1} \equiv n \cdot a^k \pmod{7}.$$

Explain why $a^k \equiv a^k \pmod{7}$, and then deduce that

$$n \cdot a^k \equiv a^{k+1} \pmod{7}.$$

(Notice that $n^{k+1} = n \cdot n^k$ and $a^{k+1} = a \cdot a^k$.) Then deduce that

$$n^{k+1} \equiv a^{k+1} \pmod{7}.$$

(Notice that $n^{k+1} - a^{k+1} = (n^{k+1} - n \cdot a^k) + (n \cdot a^k - a^{k+1})$.)

(d) Explain why (c) does **not** imply that we necessarily have $n^{k+1} \equiv a^{k+1} \pmod{7}$. Explain why (c) does imply that **if** $n^k \equiv a^k \pmod{7}$ **then** $n^{k+1} \equiv a^{k+1} \pmod{7}$.

(e) Suppose n and a are integers with $n \equiv a \pmod{7}$. So from (b) we know that $n^3 \equiv a^3 \pmod{7}$. Use (d) with $k = 3$ to deduce that $n^4 \equiv a^4 \pmod{7}$.

(f) Suppose n and a are integers with $n \equiv a \pmod{7}$. So from (e) we know that $n^4 \equiv a^4 \pmod{7}$. Use (d) with $k = 4$ to deduce that $n^5 \equiv a^5 \pmod{7}$.

(g) Suppose n and a are integers with $n \equiv a \pmod 7$. So from (f) we know that $n^5 \equiv a^5 \pmod 7$. Use (d) with $k = 5$ to deduce that $n^6 \equiv a^6 \pmod 7$.

(h) Suppose n and a are integers with $n \equiv a \pmod 7$. Does (d) imply that $n^{100} \equiv a^{100} \pmod 7$? Does (d) imply that $n^{5000} \equiv a^{5000} \pmod 7$? Does (d) imply that $n^k \equiv a^k \pmod m$ for all natural numbers k? Clearly explain your reasoning.

4.6. Throughout, let m be a natural number.

(a) Suppose n and a are integers with $n \equiv a \pmod m$. Deduce that

$$n^2 \equiv n \cdot a \pmod m \qquad \text{and} \qquad n \cdot a \equiv a^2 \pmod m.$$

Then deduce that $n^2 \equiv a^2 \pmod m$. (You may want to use #4.4.)

(b) Suppose n and a are integers with $n^2 \equiv a^2 \pmod m$. Use this to deduce that

$$n^3 \equiv n \cdot a^2 \pmod m.$$

Explain why $a^2 \equiv a^2 \pmod m$, then deduce that

$$n \cdot a^2 \equiv a^3 \pmod m.$$

Then deduce that

$$n^3 \equiv a^3 \pmod m.$$

(c) Suppose that n, a and k are natural numbers. Suppose also that $n^k \equiv a^k \pmod m$. Deduce that

$$n^{k+1} \equiv n \cdot a^k \pmod m.$$

Explain why $a^k \equiv a^k \pmod m$, and then deduce that

$$n \cdot a^k \equiv a^{k+1} \pmod m.$$

(Notice that $n^{k+1} = n \cdot n^k$ and $a^{k+1} = a \cdot a^k$.) Then deduce that

$$n^{k+1} \equiv a^{k+1} \pmod m.$$

(Notice that $n^{k+1} - a^{k+1} = (n^{k+1} - n \cdot a^k) + (n \cdot a^k - a^{k+1})$.)

(d) Explain why (c) does **not** imply that we necessarily have $n^{k+1} \equiv a^{k+1} \pmod m$. Explain why (c) does imply that **if** $n^k \equiv a^k \pmod m$ **then** $n^{k+1} \equiv a^{k+1} \pmod m$.

(e) Suppose n and a are integers with $n \equiv a \pmod m$. So from (b) we know that $n^3 \equiv a^3 \pmod m$. Use (d) with $k = 3$ to deduce that $n^4 \equiv a^4 \pmod m$.

(f) Suppose n and a are integers with $n \equiv a \pmod{m}$. So from (e) we know that $n^4 \equiv a^4 \pmod{m}$. Use (d) with $k = 4$ to deduce that $n^5 \equiv a^5 \pmod{m}$.

(g) Suppose n and a are integers with $n \equiv a \pmod{m}$. So from (f) we know that $n^5 \equiv a^5 \pmod{m}$. Use (d) with $k = 5$ to deduce that $n^6 \equiv a^6 \pmod{m}$.

(h) Suppose n and a are integers with $n \equiv a \pmod{m}$. Does (d) imply that $n^{100} \equiv a^{100} \pmod{m}$? Does (d) imply that $n^{5000} \equiv a^{5000} \pmod{m}$? Does (d) imply that $n^k \equiv a^k \pmod{m}$ for all natural numbers k? Clearly explain your reasoning.

4.7. Here we find an easy way to determine whether a 3 digit number is divisible by 9.

(a) Briefly explain why $10 \equiv 1 \pmod{9}$. (**Suggestion:** Begin by translating the notation into words. What does it mean for two numbers to be congruent modulo 9?)

(b) Briefly explain why $10 \cdot 3 \equiv 1 \cdot 3 \pmod{9}$.
(**Suggestion:** Use (a) and #4.4 (m), or note that $10 \cdot 3 - 1 \cdot 3 = (10 - 1) \cdot 3$.)

(c) Explain why $10 \cdot b \equiv 1 \cdot b \pmod{9}$ where b denotes some integer.

(d) Briefly explain why $10 \cdot 3 + 7 \equiv 1 \cdot 3 + 7 \pmod{9}$. (**Suggestion:** Use (b) and #4.4 (b).)

(e) Suppose b is some integer. Explain why $10 \cdot b + 3 \equiv 1 \cdot b + 3 \pmod{9}$. (**Suggestion:** Use (c) and #4.4 (b).)

(f) Suppose a and b are integers. Explain why $10 \cdot b + a \equiv 1 \cdot b + a \pmod{9}$. (**Suggestion:** Use (c) and #4.4 (b).)

(g) Suppose a and b are integers. Explain why $10 \cdot b + a$ is divisible by 9 exactly when $b + a$ is divisible by 9. (So you must demonstrate two things: (i) If $10 \cdot b + a$ is divisible by 9 then $b + a$ is divisible by 9; and (ii) If $b + a$ is divisible by 9 then $10 \cdot b + a$ is divisible by 9. Remember what you just deduced about $(10 \cdot b + a) - (b + a)$.)

(h) Use (g) to determine whether 9 divides 51; breifly explain your reasoning. (Notice that $51 = 10 \cdot 5 + 1$.)

(i) Briefly explain why $10^2 \equiv 1^2 \pmod{9}$, then conclude that $100 \equiv 1 \pmod{9}$. (You may want to use #4.6.)

(j) Briefly explain why $100 \cdot 3 \equiv 1 \cdot 3 \pmod{9}$. (You may want to use (i) and #4.4 (j).)

(k) Explain why $100 \cdot c \equiv 1 \cdot c \pmod{9}$ where c denotes some integer. (**Suggestion:** Use (i) and #4.4 (j).)

(l) Briefly explain why $100 \cdot 3 + 10 \cdot 7 + 5 \equiv 1 \cdot 3 + 1 \cdot 7 + 5 \pmod{9}$. (**Suggestion:** Use (f), (k) and #4.4 (l).)

(m) Suppose a, b and c are integers. Explain why $100 \cdot c + 10 \cdot b + a \equiv 1 \cdot c + 1 \cdot b + a \pmod{9}$.

(p) Suppose a, b and c are integers. Explain why $100 \cdot c + 10 \cdot b + a$ is divisible by 9 exactly when $c + b + a$ is divisible by 9.

(q) Use (p) to determine whether 9 divides 513; breifly explain your reasoning.

(r) Can you extend this argument to determine whether numbers with more than 3 digits are divisible by 9? Clearly explain your reasoning.

4.8. Here we find an easy way to determine whether a 4 digit number is divisible by 11.

(a) Briefly explain why $10 \equiv -1 \pmod{11}$.

(b) Briefly explain why $10 \cdot 3 \equiv -1 \cdot 3 \pmod{11}$.

(c) Explain why $10 \cdot b \equiv -1 \cdot b \pmod{11}$ where b denotes some integer.

(d) Briefly explain why $10 \cdot 3 + 7 \equiv -1 \cdot 3 + 7 \pmod{11}$.

(e) Suppose b is some integer. Demonstrate that $10 \cdot b + 3 \equiv -1 \cdot b + 3 \pmod{11}$.

(f) Suppose a and b are integers. Explain why $10 \cdot b + a \equiv -1 \cdot b + a \pmod{11}$. (You may want to use #4.4.)

(g) Suppose a and b are integers. Demonstrate that $10 \cdot b + a$ is divisible by 11 exactly when $-b + a$ is divisible by 11. (So you must demonstrate two things: (i) If $10 \cdot b + a$ is divisible by 11 then $-b + a$ is divisible by 11; and (ii) If $-b + a$ is divisible by 11 then $10 \cdot b + a$ is divisible by 11. Remember what you have just deduced about $(10 \cdot b + a) - (-b + a)$.)

(h) Use (g) to determine whether 11 divides 51; breifly explain your reasoning. (Notice that $51 = 10 \cdot 5 + 1$.)

(i) Explain why $10^2 \equiv (-1)^2 \pmod{11}$. Conclude that $100 \equiv 1 \pmod{11}$.

(j) Briefly explain why $100 \cdot 3 \equiv 1 \cdot 3 \pmod{11}$.

(k) Explain why $100 \cdot c \equiv 1 \cdot c \pmod{11}$ where c denotes some integer.

(l) Suppose a, b and c are integers. Explain why

$$100 \cdot c + 10 \cdot b + a \equiv 1 \cdot c - 1 \cdot b + a \pmod{11}.$$

(m) Suppose a, b and c are integers. Explain why $100 \cdot c + 10 \cdot b + a$ is divisible by 11 exactly when $c - b + a$ is divisible by 11.

(n) Use (m) to determine whether 11 divides 572; breifly explain your reasoning.

(o) Explain why $10^3 \equiv (-1)^3 \pmod{11}$. Conclude that $1000 \equiv -1 \pmod{11}$.

(p) Explain why $1000 \cdot d \equiv -1 \cdot d \pmod{11}$ where d denotes some integer.

(q) Suppose a, b, c and d are integers. Explain why

$$1000 \cdot d + 100 \cdot c + 10 \cdot b + a \equiv -1 \cdot d + 1 \cdot c - 1 \cdot b + a \pmod{11}.$$

(r) Suppose a, b, c and d are integers. Explain why

$$1000 \cdot d + 100 \cdot c + 10 \cdot b + a$$

is divisible by 11 exactly when

$$-d + c - b + a$$

is divisible by 11.

(s) Use (r) to determine whether 11 divides 8391; breifly explain your reasoning.

(t) Can you extend this argument to determine whether numbers with more than 4 digits are divisible by 11? Clearly explain your reasoning.

4.9. **Recall:** Given any integer n, there is an integer s and a whole number t so that $n = 7 \cdot s + t$ where t is smaller than 7.

(a) Find an integer s and a whole number t so that $-25 = 7 \cdot s + t$ where t is smaller than 7. (So t is either $0, 1, 2, 3, 4, 5$ or 6.) Then, with this choice of t, explain why $-25 \equiv t \pmod 7$.

(b) Let n denote an integer. Explain why $n \equiv t \pmod 7$ where t is either $0, 1, 2, 3, 4, 5$ or 6.

(c) Using (b), briefly explain why, given any integers k and m, $k \cdot m \equiv t \pmod 7$ where t is either $0, 1, 2, 3, 4, 5$ or 6.

(d) Suppose k and m denote whole numbers between 0 and 6. By (c), we know $k \cdot m$ is congruent modulo 7 to some whole number between 0 and 6. For instance, $5 \cdot 2 \equiv 3 \pmod 7$, and $3 \cdot 6 \equiv 4 \pmod 7$. Complete the attached multiplication table modulo 7 so that each entry in the table is a whole number between 0 and 6.

(e) Suppose c denotes an integer. Explain why $c \cdot 3 \equiv c \cdot 10 \pmod 7$, and why $3 \cdot c \equiv 10 \cdot c \pmod 7$.

(f) Suppose a, b and c denote integers, and suppose $a \equiv b \pmod 7$. Using the definition of congruence, explain why $c \cdot a \equiv c \cdot b \pmod 7$, and why $a \cdot c \equiv b \cdot c \pmod 7$.

(g) Suppose k, m and n denote integers; suppose also that $k \equiv m \pmod 7$ and $m \equiv n \pmod 7$. Deduce that $k \equiv n \pmod 7$. (**Suggestion:** Notice that $n - k = (n - m) + (m - k)$.)

(h) Use (d) to find a whole number k between 0 and 6 so that $k \cdot 3 \equiv 1 \pmod 7$. Using (f), deduce that $k \cdot 3 \cdot x \equiv x \pmod 7$.

(i) Suppose $3 \cdot x \equiv 2 \pmod 7$ where x is a whole number between 0 and 6. Taking k as in (h), multiply both sides of the above congruence by k, obtaining $k \cdot 3 \cdot x \equiv k \cdot 2 \pmod 7$. Use this to find the value of x. (Remember that x is between 0 and 6.)

4.10. **Recall:** Given any integer n, there is an integer s and a whole number t so that $n = 6 \cdot s + t$ where t is smaller than 6.

(a) Find an integer s and a whole number t so that $-25 = 6 \cdot s + t$ where t is smaller than 6. (So t is either $0, 1, 2, 3, 4$ or 5.) Then, with this choice of t, explain why $-25 \equiv t \pmod 6$.

(b) Let n denote an integer. Explain why $n \equiv t \pmod 6$ where t is either $0, 1, 2, 3, 4$ or 5.

(c) Using (b), briefly explain why, given any integers k and m, $k \cdot m \equiv t \pmod 6$ where t is either $0, 1, 2, 3, 4$ or 5.

(d) Suppose k and m denote whole numbers between 0 and 5. By (c), we know $k \cdot m$ is congruent modulo 6 to some whole number between 0 and 5. For instance, $5 \cdot 2 \equiv 4 \pmod 6$, and $2 \cdot 4 \equiv 2 \pmod 6$. Complete the attached multiplication table modulo 6 so that each entry in the table is a whole number between 0 and 5.

(e) Suppose c denotes an integer. Explain why $c \cdot 5 \equiv c \cdot 11 \pmod 6$, and why $5 \cdot c \equiv 11 \cdot c \pmod 6$.

(f) Suppose a, b and c denote integers, and suppose $a \equiv b \pmod 6$. Using the definition of congruence, explain why $c \cdot a \equiv c \cdot b \pmod 6$, and why $a \cdot c \equiv b \cdot c \pmod 6$.

(g) Suppose k, m and n denote integers; suppose also that $k \equiv m \pmod 6$ and $m \equiv n \pmod 6$. Deduce that $k \equiv n \pmod 6$. (**Suggestion:** Notice that $n - k = (n - m) + (m - k)$.)

(h) Use (l) to find a whole number k between 0 and 5 so that $k \cdot 5 \equiv 1 \pmod 6$. Using (f), deduce that $k \cdot 5 \cdot x \equiv x \pmod 6$.

(i) Suppose $5 \cdot x \equiv 2 \pmod 6$ where x is a whole number between 0 and 5. Taking k as in (h), multiply both sides of the above congruence by k, obtaining $k \cdot 5 \cdot x \equiv k \cdot 2 \pmod 6$. Use this to find the value of x. (Remember that x is between 0 and 5.)

(j) Suppose $a \equiv b \pmod 6$ for integers a, b. Deduce that $a \equiv b \pmod 3$ and $a \equiv b \pmod 2$.

(t) Suppose $3 \cdot x \equiv 2 \pmod 6$ where x is a whole number between 0 and 5. Either find the value of x, or explain why no such x exists.

Appendix
Assumptions, Definitions, Terminology and Notation

Assumptions: We agree we understand what the numbers $1, 2, 3, 4, 5$, *etc.* represent. (The latin abbreviation "*etc.*" indicates that the list extends indefinitely.) These numbers are called the *counting numbers*, since we use them to count things; they are also called the *natural numbers*, since they arise naturally in our lives. We also agree that, given a (finite) collection of objects, the number of objects we have does not depend on the order in which we count them. Also, we agree we understand what it means for one natural number to be larger or smaller than another. Also, we assume that when we add together two natural numbers, we obtain another natural number. For instance, $3 + 5$ is 8, which is another natural number.

A definition of addition: Imagine drawing 3 dots of one color followed by 5 dots of another color; we agree that $3 + 5$ is the total number of dots. More generally, let m and n represent natural numbers. Imagine drawing m dots of one color followed by n dots of another color; we agree that $m + n$ is the total number of dots.

Another assumption: We assume that when we add together two natural numbers, we obtain another natural number. For instance, $3 + 5$ is 8, which is another natural number.

Notation: We sometimes use parentheses to indicate in which order to perform operations. For instance, the expression $(3 + 5) + 9$ denotes the number we obtain by first adding 3 to 5, then adding 9 to the result. (So $(3 + 5) + 9$ is the same as $8 + 9$.) Pictorially, $(3 + 5) + 9$ denotes the number of dots we have when we have $3 + 5$ dots followed by 9 dots. Similarly, $3 + (5 + 9)$ denotes the number we obtain by adding 3 to the number obtained by adding 5 to 9. (So $3 + (5 + 9)$ is the same as $3 + 14$.) Pictorially, $3 + (5 + 9)$ denotes the number of dots we have when we have 3 dots followed by $5 + 9$ dots.

A definition of multiplication: The expression $5 \cdot 8$ refers to the quantity obtained by taking 5 copies of 8 objects. More generally, say m and n represent natural numbers; the expression $m \cdot n$ refers to the quantity obtained by taking m copies of n objects.

Another assumption: We assume that when we multiply together two natural numbers, we obtain another natural number. For instance, $5 \cdot 8$ is 40, another natural number.

Notation: The notation $(3 \cdot 5) \cdot 9$ refers to the quantity obtained by muliplying $3 \cdot 5$ by 9. (So $(3 \cdot 5) \cdot 9$ is the same as $15 \cdot 9$.) Similarly, $3 \cdot (5 \cdot 9)$ denotes the quantity obtained by multiplying 3 by the quantity $5 \cdot 9$. (So $3 \cdot (5 \cdot 9)$ is the same as $3 \cdot 45$.) More generally, with k, m and n denoting natural numbers, $(k \cdot m) \cdot n$ denotes the quantity obtained by multiplying the quantity $k \cdot m$ with n. Similarly, $k \cdot (m \cdot n)$ denotes the quantity obtained

by multiplying k by the quantity $m \cdot n$.

Notation: When two expressions denote the same quantity, we say they are equal. We use the symbol $=$ to mean "is equal to."

Terminology: Since $24 = 6 \cdot 4$, we say 24 is divisible by 6. We also say that 6 divides 24, and that 6 is a divisor of 24. Similarly, since $27 = 9 \cdot 3$, we say 27 is divisible by 9, and 9 is a divisor of 27. More generally, when n is a natural number that is equal to 6 times another natural number (i.e.

$$n = 6 \cdot k$$

for some natural number k), we say that n is divisible by 6 and that 6 is a divisor of n. More generally still, when m and n are natural numbers and n is equal to m times another natural number (i.e.

$$n = m \cdot k$$

for some natural number k), we say that n is divisible by m and that m is a divisor of n.

A definition of subtraction: Suppose we have 5 objects, then we subtract, or remove, 3 of these objects; the remaining number of objects is denoted by $5 - 3$. Pictorially, imagine drawing 5 dots, then crossing out 3 dots; the remaining number of dots is $5 - 3$. More generally, suppose we have n objects where n is a natural number at least as big as 3, and then we remove 3 of the objects; the remaining number of ojects is $n - 3$. Pictorially, suppose we draw n dots and then we cross out 3 dots; the remaining number of dots is $n - 3$. More generally still, suppose we have n objects, where n is a natural number, and then we remove k of the objects where k is a natural number not exceeding n; the remaining number of objects is $n - k$.

Another assumption: Suppose k and n are natural numbers, and suppose k is smaller than n. Then we assume that $n - k$ is another natural number. For instance, 5 and 3 are natural numbers and 3 is smaller than 5; $5 - 3$ is 2, which is another natural number.

Terminology: The numbers

$$0, 1, -1, 2, -2, 3, -3, 4, -4, 5, -5, \ldots$$

are called the integers. The numbers

$$-1, -2, -3, -4, -5, \ldots$$

are called the negative integers.

More assumptions: Negative numbers are often useful to express orientation, i.e. to distinguish forward from reverse. We interpret the symbol $-$ to mean "in reverse." So for

instance, imagine being on a very long, straight path where a forward direction is indicated. To take 5 steps, we move forward 5 steps. To take -5 steps, we move **in reverse** 5 steps (so we move **backward** 5 steps). Notice that when you take 7 steps then -3 steps (i.e. when you move forward 7 steps then backward 3 steps), then you are in the same place as when you take -3 steps then 7 steps. Similarly, when you take 5 steps then -12 steps, then you are in the same place as when you take -12 steps then 5 steps. More generally, we assume that, for x and y integers, when you take x steps then y steps, you are in the same place as when you take y steps then x steps. So we are assuming addition of integers is commutative, i.e. $x+y = y+x$ for any integers x and y. Also, when you take $\big(7+(-3)\big)$ steps followed by 5 steps, you are in the same place as when you take 7 steps followed by $\big((-3)+5\big)$ steps. More generally, we assume that addition of integers is associative, i.e. $(x+y)+z = x+(y+z)$ for any integers x, y and z.

Terminology: We say that 3 divides -12 (or equivalently, that 3 is a divisor of -12 or that -12 is divisible by 3) since $-12 = 3 \cdot (-4)$. More generally, we say that 3 divides an integer n if $n = 3 \cdot q$ for some integer q. More generally still, we say that an integer m divides another integer n if $n = m \cdot q$ for some integer q.

Terminology: We call a natural number even when it is divisible by 2. The odd natural numbers are those not divisible by 2. So the odd natural numbers are between the even natural numbers, and thus each even natural number is preceded by an odd natural number.

Notation: When a natural number n is even, we write $\frac{1}{2} \cdot n$ to denote half of n. For instance, $\frac{1}{2} \cdot 6 = 3$, and $\frac{1}{2} \cdot 10 = 5$. More generally, if n is even then $n = 2 \cdot k$ for some natural number k; then

$$\frac{1}{2} \cdot n = k.$$

Terminology: Since each natural number n is equal to $1 \cdot n$, 1 is called a multiplicative identity. A natural number greater than 1 is called prime if it is divisible only by 1 and itself. (For example, 2, 3, 7 and 17 are prime; 15 and 9 are not.)

Terminology: We say a natural number d is a divisor of another natural number n if n is divisible by d, i.e. $n = d \cdot k$ for some natural number k. We say d is a common divisor of m and n if d is both a divisor of m and of n. We say a common divisor d of m and n is the greatest common divisor if d is larger than every other common divisor of m and n.

Abbreviation: "gcd" stands for "greatest common divisor."

Notation: Given integers a, b, the notation $a \equiv b \pmod 7$ means that 7 divides $a-b$. For instance, $3 \equiv 10 \pmod 7$ and $-12 \equiv 5 \pmod 7$. More generally, given a natural number

m and integers a, b, the notation $a \equiv b \pmod{m}$ means that m divides $a - b$. (The symbol $\equiv$ is shorthand for "is congruent to", and "mod" is shorthand for "modulo".)

Notation: We write n^2 to denote $n \cdot n$, n^3 to denote $n \cdot n \cdot n$, n^4 to denote $n \cdot n \cdot n \cdot n$, etc.