Introduction to Number Theory With Applications to Middle School Mathematics and Cryptography

Supplementary materials

For MTHT 467, University of Illinois at Chicago

Bonnie Saunders, Spring 2012

This is a first draft version of workbook/text for MTHT 467: Introduction to Number Theory with applications to Middle School Mathematics and Cryptography. This is the version used in Spring 2012 and is currently being updated. As much as possible teaching notes are in blue. Assorted answers are in red. Colored comments are not printed for students.

Table of Contents

Chapter 5 General Substitution Ciphers Keyword Cipher
BIG IDEA: Frequency analysis Cracking Substitution
37 Substitution Tables: Inverses?
38 Counting: How many cipher tables are there?
39 Teaching Presentation option
40 Cryptography in Spanish: Frequency analysis Webpage Cipher Tools
41 Computing Frequencies: Spanish Rogue Computer
43 Guess the keyword (2 examples**Factoring from CryptoClub Book**Vigenère Cipher

Chapter 6 Euclidean Algorithm
BIG IDEA: The Euclidean Algorithm
45 Factors: Definitions and Examples
46 gcd and problems
47 lcm and problems Cracking Numbernames
48 Crickets and Chinese Remainder
49 Finding gcd without factoring
50 The Euclidean Algorithm WolframAlpha
51 Practice with the Euclidean Algorithm
52 Geometry and the Euclidean Algorithm

Math in Context: Looking at Combinations **Presentations: Combination problems**
Chapter 7 Extended Euclidean Algorithm
BIG IDEA: Extended Euclidean Algorithm Excel worksheets
53 Combination charts
55 Combination Chart Problems
57 Solving Ax + By = gcd(A,B)
59 Extended Euclidean Algorithm Worksheet program for TI-84
60 TI-84 program
61 More Diophantine Equations to Solve
62 More Combination Problems
63 Combination Problems with Negative Numbers

Modular Arithmetic from CryptoClub book
Applications of Modular Arithmetic **Presentations: Calendar problems**
Chapter 8 Modular Arithmetic
BIG IDEA: modular arithmetic Multiplicative cracking
65 Modular Arithmetic: Reducing mod *m* Affine Ciphers
67 Modular Arithmetic: Rules
69 Modular Arithmetic: More Congruence Equations
70 Modular Arithmetic: Common Factors
71 Modular Arithmetic: Divisibility Rules Explained
72 Modular Arithmetic: Finding Multiplicative Inverses
73 4-digit Multiplicative Cipher: mod 10000
75 4-digit Multiplicative Cipher: mod 9999
76 4-digit Multiplicative Cipher: Finding Inverses
77 4-digit Multiplicative Cipher: Project
78 Presentation Idea

Prime Numbers from CryptoClub Book **Presentations: Prime activities**

Chapter 9 Prime Numbers

BIG IDEA: Prime numbers

79 Finding primes without factoring: Sieve of Eratosthenes
81 Primes to 10000 without factoring
82 There is an Infinite Number of Primes
83 Unique Prime Factorization

Chapter 10 Power Ciphers **Presentations: CME Exponents**

BIG IDEA: exponents

85 Power Ciphers
86 Finding Patterns in Power Cipher Tables
88 Power Cipher Mod 37
89 Fermat's little theorem
90 Power Cipher Mod 55
91 Power Cipher mod 437
92 Power Cipher: Using Larger Mods
93 Power Ciphers: RSA Encryption

Goals of MTHT 467

Upon completing this course you will

1. Be a qualified CryptoClub Leader. You will learn how cryptography can support the learning of middle school math skills and how to make learning mathematics fun and engaging.

2. Understand college level number theory and it's applications to cryptography, including
    a. Extended Euclidean Algorithm
    b. Solving Diophantine Equations
    c. Modular Arithmetic
    d. Prime Numbers
    e. RSA encryption

3. Increase awareness of the role of number theory ideas in middle school. You will know how to reason and explain
    a. Negative Numbers
    b. Solving linear equations
    c. Factoring, lcm, gcd
    d. Prime numbers
    e. frequency analysis
    f. exponentials
    g. functions and inverses
    h. and more . . .

Ciphers and Functions

Definition: A function is a rule that assigns every element of one set, called the domain, to a unique element of another set, called the range.

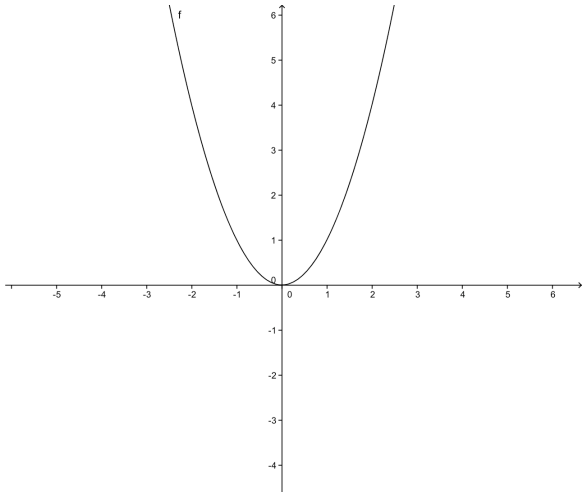
Examples: You may be used to thinking of functions where the domain and range are both the set of all real numbers. You may think of this kind of function as being given by a formula like

$f(x) = x^2$ or $g(x) = 3x - 5$

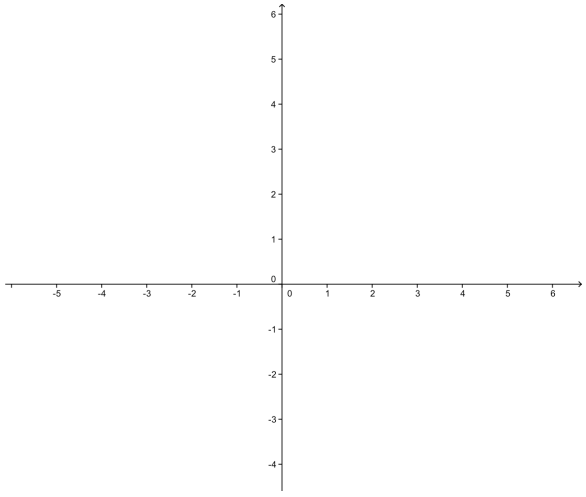
But there can be functions that map between different kinds of sets. For example, the Caesar cipher with key=k is a function. The domain and range for this function are the same: the set of letters of the alphabet. In the Student Cipher Handbook the domain is called plaintext, and written with lowercase letters of the alphabet and the range is called ciphertext and written in uppercase letters. In this section we investigate different ciphers and describe them in terms of functions using function notation and vocabulary.

A function can be represented by a graph. This is the set of all pairs $(x, f(x))$ for every value of in the domain of the function.

The graph of $f(x) = x^2$ looks like:

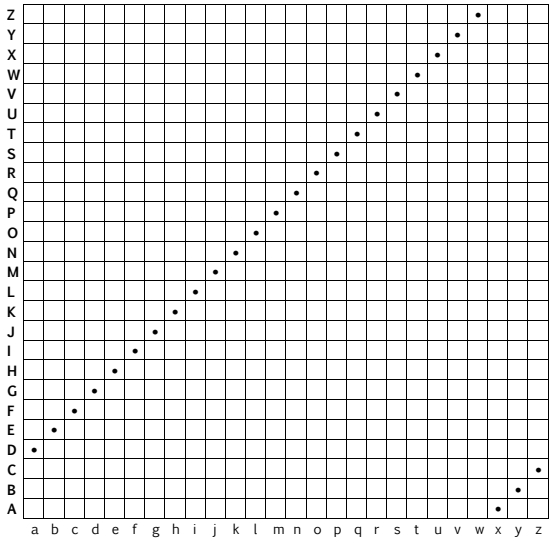


Sketch the graph of $g(x) = 3x - 5$:

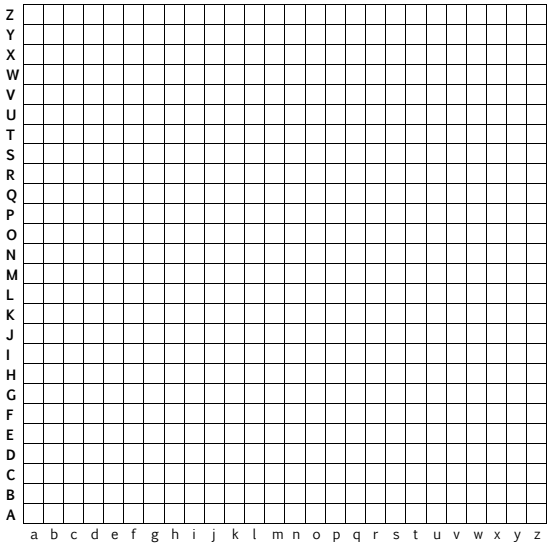


Use this space to record differences you see in these two graphs:

The Caesar Cipher with key = 3 is represented by a graph that looks like this:



Sketch a graph that represents Caesar Cipher with key = 16



Each square with a dot tells which plaintext letter (along the x-axis) maps to which CIPHRTEXT letter (along the *y*-axis).

If the domain of a function is a finite set the function can also be represented by an input-output table. The inputs are all the values in the domain and the outputs are the corresponding assigned values in the range. *A cipher table is an input-output table.*

> A function is said to be **one-to-one** (or **1-1**) if each value of the function comes from *exactly one* element of the domain.

Examples: The function $f(x) = x^2$, with domain = range = all real numbers, is not one-to-one because there are two values that map to any positive number. For example, -2 and 2 both map to 4. That is $f(-2) = f(2)$. The function $g(x) = 3x - 5$ is one-to-one: For any real number in the range, (say 10) we can solve an equation (like, $3x - 5 = 10$) to find out that only one number in the domain gets mapped to that number from the range. (In our example, x must be 5. No other number gets mapped to 10.) In other words, if $g(a) = g(b)$, then $a = b$.

Example: Any Caesar Cipher is one-to-one because each CIPHERTEXT letter represents exactly one plaintext letter. In fact, a good cipher must be 1-1. Otherwise one could never decrypt.

> A function is said to be **onto** if every value in the range is realized as a value of the function.

Example: The function $f(x) = x^2$, with domain = range = all real numbers, is not onto because, for example, -3 is not the square of any real number. One could limit the definition and say that the range is just the non-negative numbers. Then the function, with this new domain, is onto. Whether or not a unction can depend on the stated range of the function.

Example: Any Caesar Cipher is onto because every letter in the alphabet is a possible CIPHERTEXT letter.

Three problems with functions.

In algebra there are three different problems that students learn to do with a function:

1. Evaluate the function at a value for x.
2. Solve for x given a particular value of the function.
3. Given specific x, $f(x)$ values, find the function.

These problems are universal throughout mathematics. They appear over and over again in different situations and various guises. They form the bases for learning cryptography as well. Consider the two examples of each type of problem listed below:

Evaluate the function:

If $f(x) = 2x + 5$, what is $f(2)$?

Using Caesar cipher key = 5,
ENCRYPT the word: c r y p t o

Solve for x:

If $f(x) = 2x + 5$, what value(s) of x make $f(x) = 10$?

This word was encrypted using Caesar Cipher, key = 5
DECRYPT: H F J X F W

Find the function:

If $f(x) = mx + b$, what values of m and b make the graph of f a straight line through the points (0, 0) and (1, 2)?

This word was encrypted using a Caesar Cipher. What is the key?
CRACK: C B M M P P O

It may seem that the order given here is the natural order in which to learn how to do these three problems. However, even in elementary school, the problems may appear in a different order. Consider the following sequence of questions, in which finding a formula for the function is the ultimate goal

1. Find a possible pattern and continue this list of numbers: 1, 4, 7, 10, . . .
   Students see to add 3 to continue the sequence for many more terms.
2. What is 10^{th} number on the list? What is the 100^{th} number on the list?
   Student identify the 10^{th} number from the list they generated. However, it will be long and tedious to find the 100^{th} term by extending the sequence. This motivates looking for a formula.
3. Is the number 25 on the list? Is the number 127 on the list?
   Students find 25 on their list. Deciding whether or not larger numbers are on the list encourages students to see the sequence numbers as 1 more than a multiple of three.
4. What is a formula for the n^{th} number on the list?
   Student most likely need teacher guidance to see the formula is $3(n-1)+1$. Seeing how this work will unfold after many similar problems are worked. Students need to understand multiplication as repeated addition. Problems like #3 help students understand the rationale of the formula.

Likewise in Cryptography, we often start with a cracking problem to investigate the pattern of a new cipher. Giving students time to explore possible patterns is a valuable way to learn about functions.

Inverses -- Under development.

Decrypting is the inverse operation to encrypting.

There are many different kinds of inverses in mathematics.

Subtracting is the inverse operation of adding. Dividing is the inverse operation of multiplying by a non-zero number.

Some operations that don't have inverses. For example, multiplying by 0 or squaring a number.

Example: If we think of a function as operating on values in the domain to give values in the range. We can wonder if we can inverse the operation. The function $g(x) = 3x - 5$ has an inverse. The operation of g can be recorded as first multiply by 3 then subtract 5. To do the inverse we would first add 5 ad then divide by 3. This is exactly what we might do to solve an equation like

$$3x - 5 = 10$$

Solving equations: Minds in Action pg 120. backtracking to solve equations.

Letter-to-Number: Numbernames

a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z
00	01	02	03	04	05	06	07	08	09	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25

Code your name in numbers. If your name is long, just use the first five letters in your name. If your name is too short, add some letters from your last name to make five letters in all.

Example: **Your name**:

c	a	t	h	y																	
2	0	19	7	24																	

You can further encode your ***numbername*** as one number by pushing all of the numbers together. When doing this first add a zero in front of each single digit. Cathy's name in numbers is

02-00-19-07-24 and her numbername is 0200190724.

If the extra zeros were not there we could not tell who it was; 2019724 could be 20-19-7-24 (decodes to uthy) or it might be 2-01-9-7-2-4 (decodes to cbjhce).

1. Write your numbername: _____

NOTE: If Cathy doesn't put the zero in front of her name then we have to count the number of digits to figure out that the first letter-number is 2 and not 20.

2. Decode these numbernames to names:

900120418 11080204 10800130300

A word about functions: Numbername maps names to integers. It is a function because each name maps to one and only one number. The function is not 1-1. For example, "Lice" and Alice" map to the same number. This means that it requires some educational guessing to figure out the message. The function is not onto. Numbers with a "99" in them, for example, do not come from strings of letters. A clever cryptographer may observe and use this information to help crack a code.

Secret Numbernames There are many ways you might encrypt your numbername to keep it a secret. Here is a way that is not commonly used but still works: Just multiply your numbername by any other number, say 3. Only tell your friends which number you multiplied by.

Example: Cathy's name becomes 200190724 X 3 = 600572172

3. Pick another number. Multiply your numbername by it and write the result here:

4. Is this cipher 1-1? Is it onto?

5. **Cracking numbernames**. Six people encrypted their numbernames by multiplying by a number. They all used the same number so they could use it to send secret messages. These are the encrypted names. Can you figure out what number they used. What are their names?

156022412 14484610634 24754232412 1706952 1405444612

6. Factor your numbername. Is your numbername easy or hard to factor?

Numbernames with smaller numbers: Another thing to do with your numbername is to treat each number separately. For example we could multiply each letter in Cathy's number name by 7 and get the five numbers:

14 – 00 – 133 – 49 – 168

[Notice: We need to provide separators for the numbers because cipher numbers are not necessarily two digit numbers.]

7. Is this cipher that maps the numbers from 0 to 26 to numbers 1-1? Is it onto?

8. Figure out the numbername and what number was used to encyrpt it:

216 – 9912 – 96

9. Pick a number. Encrypt your numbername by multiplying each letter by that number. Use these encrypted names to play Cipher Tag.

10. Is this cipher 1-1? Is it onto?

Additive Cipher: 36-letter alphabet

If you increase the characters allowed in your alphabet you increase the possibilities in your messages. Here is a possible coding that let's you decrypt numbers as well as letters.

0	1	2	3	4	5	6	7	8	9	a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z
00	01	02	03	04	05	06	07	08	09	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31	32	33	34	35

Examples:
Encrypt with the Additive Cipher Key = 12

plaintext:	m	t	h	t	4	6	7
encode:	22						
CIPHERNUMBER:	24						

Decrypt this message that was encrypted using the Additive Cipher, Key = 33

plaintext:	2												
decode:	02												
CIPHERNUMBER:	35	35	34	8		8	7	17	11	24			

1. Encrypt your street address using an additive cipher. Use the key of your choice.

plaintext:																		
encode:																		
CIPHERNUMBER:																		

2. Which of the following numbers are prime numbers? Each number was encode, digit by digit, with the 36-letter alphabet and then encrypted with an additive cipher. the key given is the encryption key.

1018, Key=9 161922, Key=15 350233, Key=30 17251619, Key unknown

3. Crack the additive code and decrypt this arithmetic statement:

1 2 1 7 0 4 2 9 3 3 2 5 0 3 1 3 1 4 2 9 0 3 1 4 1 7 1 9

Sideways Arithmetic

Here are some fun arithmetic puzzles that use a different kind of coding. In each arithmetic problem, each digit, 0, 1, 2, 3, 4, 5, 6, 7, 8 and 9, has been replaced by a letter of the alphabet. Part of the fun is that the numbers now spell words. The book, **More Sideways Arithmetic From Wayside School** by Louis Sachar tells a story and explains how to do these problems.

These codes are functions that map digits to letters. The *domain* of each is some subset of {0,1,2,3,4,6,7,8,9}. The range is the alphabet. As a function from the digits to the alphabet each code is 1-1, but not onto.

Examples*:

1.

```
  boys
+ boys
 silly
```

input:	0	1	2	3	4	5	6	7	8	9
output:										

2.

```
  girls
+ girls
  silly
```

input:	0	1	2	3	4	5	6	7	8	9
output:										

3.

```
  arcs
+ bras
 crass
```

input:	0	1	2	3	4	5	6	7	8	9
output:										

4.

```
 llama
- seal
  seal
```

input:	0	1	2	3	4	5	6	7	8	9
output:										

* All puzzles on these two page come from the **More Sideways Arithmetic From Wayside School** by Louis Sachar

More Sideways Problems

You may want to make your own input-output table for each problem.

5.
```
  lip
+ lit
 pipe
```

6.
```
  pep
+ pen
 erne
```

7.
```
  good
+  dog
 fangs
```

8.
```
  too
  too
  too
+ too
  hot
```

9.
```
   her
+ hurl
 sells
```

10.
```
 spit
+ sip
 tips
```

11.
```
  pet
  pet
+ pet
 tape
```

12.
```
  yea
+ yay
  aye
```

13.
```
  still
  stall
+ stilt
 nitwit
```

Introduction to Coding

ASCII Code

Decimal	Octal	Hexadecimal	Binary	Symbol		Decimal	Octal	Hexadecimal	Binary	Symbol
000	000	00	00000000	NUL		064	100	40	01000000	@
001	001	01	00000001	SOH		065	101	41	01000001	A
002	002	02	00000010	STX		066	102	42	01000010	B
003	003	03	00000011	ETX		067	103	43	01000011	C
004	004	04	00000100	EOT		068	104	44	01000100	D
005	005	05	00000101	ENQ		069	105	45	01000101	E
006	006	06	00000110	ACK		070	106	46	01000110	F
007	007	07	00000111	BEL		071	107	47	01000111	G
008	010	08	00001000	BS		072	110	48	01001000	H
009	011	09	00001001	HT		073	111	49	01001001	I
010	012	0A	00001010	LF		074	112	4A	01001010	J
011	013	0B	00001011	VT		075	113	4B	01001011	K
012	014	0C	00001100	FF		076	114	4C	01001100	L
013	015	0D	00001101	CR		077	115	4D	01001101	M
014	016	0E	00001110	SO		078	116	4E	01001110	N
015	017	0F	00001111	SI		079	117	4F	01001111	O
016	020	10	00010000	DLE		080	120	50	01010000	P
017	021	11	00010001	DC1		081	121	51	01010001	Q
018	022	12	00010010	DC2		082	122	52	01010010	R
019	023	13	00010011	DC3		083	123	53	01010011	S
020	024	14	00010100	DC4		084	124	54	01010100	T
021	025	15	00010101	NAK		085	125	55	01010101	U
022	026	16	00010110	SYN		086	126	56	01010110	V
023	027	17	00010111	ETB		087	127	57	01010111	W
024	030	18	00011000	CAN		088	130	58	01011000	X
025	031	19	00011001	EM		089	131	59	01011001	Y
026	032	1A	00011010	SUB		090	132	5A	01011010	Z
027	033	1B	00011011	ESC		091	133	5B	01011011	[
028	034	1C	00011100	FS		092	134	5C	01011100	\
029	035	1D	00011101	GS		093	135	5D	01011101	]
030	036	1E	00011110	RS		094	136	5E	01011110	^
031	037	1F	00011111	US		095	137	5F	01011111	_
032	040	20	00100000			096	140	60	01100000	`
033	041	21	00100001	!		097	141	61	01100001	a
034	042	22	00100010	"		098	142	62	01100010	b
035	043	23	00100011	#		099	143	63	01100011	c
036	044	24	00100100	$		100	144	64	01100100	d
037	045	25	00100101	%		101	145	65	01100101	e
038	046	26	00100110	&		102	146	66	01100110	f
039	047	27	00100111	'		103	147	67	01100111	g
040	050	28	00101000	(		104	150	68	01101000	h
041	051	29	00101001	)		105	151	69	01101001	i
042	052	2A	00101010	*		106	152	6A	01101010	j
043	053	2B	00101011	+		107	153	6B	01101011	k
044	054	2C	00101100	,		108	154	6C	01101100	l
045	055	2D	00101101	-		109	155	6D	01101101	m
046	056	2E	00101110	.		110	156	6E	01101110	n
047	057	2F	00101111	/		111	157	6F	01101111	o
048	060	30	00110000	0		112	160	70	01110000	p
049	061	31	00110001	1		113	161	71	01110001	q
050	062	32	00110010	2		114	162	72	01110010	r
051	063	33	00110011	3		115	163	73	01110011	s
052	064	34	00110100	4		116	164	74	01110100	t
053	065	35	00110101	5		117	165	75	01110101	u
054	066	36	00110110	6		118	166	76	01110110	v
055	067	37	00110111	7		119	167	77	01110111	w
056	070	38	00111000	8		120	170	78	01111000	x
057	071	39	00111001	9		121	171	79	01111001	y
058	072	3A	00111010	:		122	172	7A	01111010	z
059	073	3B	00111011	;		123	173	7B	01111011	{
060	074	3C	00111100	<		124	174	7C	01111100	|
061	075	3D	00111101	=		125	175	7D	01111101	}
062	076	3E	00111110	>		126	176	7E	01111110	~
063	077	3F	00111111	?		127	177	7F	01111111	delete

Decoding with the ASCII Code

All text must be converted to strings of 1's and 0's in order to be stored in a computer. Use the ascii code, shown on the previous page to decode this sentence. It may be helpful to draw dividing lines on this page to help read the strings of 1's and 0's. Only decode enough to tell you what the sentence says and to determine who first wrote the words.

When you are done, encode the same words with octal code and then with hexidecimal code.

0 1 0 0 0 1 1 0 0 1 1 0 1 1 1 1 0 1 1 1 0 1 0 1 0 1 1 1 0 0 1 0 0 0 1 0 0 0 0 0 0 0 1 1 1 0 0 1 1

0 1 1 0 0 0 1 1 0 1 1 0 1 1 1 1 0 1 1 1 0 0 1 0 0 1 1 0 0 1 0 1 0 0 1 0 0 0 0 0 0 1 1 0 0 0 0 1

0 1 1 0 1 1 1 0 0 1 1 0 0 1 0 0 0 0 1 0 0 0 0 0 0 0 1 1 1 0 0 1 1 0 1 1 0 0 1 0 1 0 1 1 1 0 1 1 0

0 1 1 0 0 1 0 1 0 1 1 0 1 1 1 0 0 0 1 0 0 0 0 0 0 0 1 1 1 1 0 0 1 0 1 1 0 0 1 0 1 0 1 1 0 0 0 0 1

0 1 1 1 0 0 1 0 0 1 1 1 0 0 1 1 0 0 1 0 0 0 0 0 0 0 1 1 0 0 0 0 1 0 1 1 0 0 1 1 1 0 1 1 0 1 1 1 1

0 0 1 0 0 0 0 0 0 1 1 0 1 1 1 1 0 1 1 1 0 1 0 1 0 1 1 1 0 0 1 0 0 0 1 0 0 0 0 0 0 0 1 1 0 0 1 1 0

0 1 1 0 0 0 0 1 0 1 1 1 0 1 0 0 0 1 1 0 1 0 0 0 0 1 1 0 0 1 0 1 0 1 1 1 0 0 1 0 0 1 1 1 0 0 1 1

0 0 1 0 0 0 0 0 0 1 1 0 0 0 1 0 0 1 1 1 0 0 1 0 0 1 1 0 1 1 1 1 0 1 1 1 0 1 0 1 0 1 1 0 0 1 1 1

0 1 1 0 1 0 0 0 0 1 1 1 0 1 0 0 0 0 1 0 0 0 0 0 0 1 1 0 0 1 1 0 0 1 1 0 1 1 1 1 0 1 1 1 0 0 1 0

0 1 1 1 0 1 0 0 0 1 1 0 1 0 0 0 0 0 1 0 0 0 0 0 0 1 1 0 1 1 1 1 0 1 1 0 1 1 1 0 0 0 1 0 0 0 0 0

0 1 1 1 0 1 0 0 0 1 1 0 1 0 0 0 0 1 1 0 1 0 0 1 0 1 1 1 0 0 1 1 0 0 1 0 0 0 0 0 0 1 1 0 0 0 1 1

0 1 1 0 1 1 1 0 1 1 0 1 1 1 0 0 1 1 1 0 1 0 0 0 1 1 0 1 0 0 1 0 1 1 0 1 1 1 0 0 1 1 0 0 1 0 1

0 1 1 0 1 1 1 0 0 1 1 1 0 1 0 0 0 0 1 0 1 1 0 0 0 0 1 0 0 0 0 0 0 0 1 1 0 0 0 0 1 0 0 1 0 0 0 0

0 1 1 0 1 1 1 0 0 1 1 0 0 1 0 1 0 1 1 1 0 1 1 1 0 0 1 0 0 0 0 0 0 1 1 0 1 1 1 0 0 1 1 0 0 0 0 1

0 1 1 1 0 1 0 0 0 1 1 0 1 0 0 1 0 1 1 0 1 1 1 1 0 1 1 0 1 1 1 0 0 0 1 0 1 1 0 0 0 0 1 0 0 0 0 0

0 1 1 0 0 0 1 1 0 1 1 0 1 1 1 1 0 1 1 0 1 1 1 0 0 1 1 0 0 0 1 1 0 1 1 0 0 1 0 1 0 1 1 0 1 0 0 1

0 1 1 1 0 1 1 0 0 1 1 0 0 1 0 1 0 1 1 0 0 1 0 0 0 0 1 0 0 0 0 0 0 1 1 0 1 0 0 1 0 1 1 0 1 1 1 0

0 0 1 0 0 0 0 0 0 1 0 0 1 1 0 0 0 1 1 0 1 0 0 1 0 1 1 0 0 0 1 0 0 1 1 0 0 1 0 1 0 1 1 1 0 0 1 0

0 1 1 1 0 1 0 0 0 1 1 1 1 0 0 1 0 0 1 0 1 1 0 0 0 0 1 0 0 0 0 0 0 1 1 0 0 0 0 1 0 1 1 0 1 1 1 0

0 1 1 0 0 1 0 0 0 0 1 0 0 0 0 0 0 1 1 0 0 1 0 0 0 1 1 0 0 1 0 1 0 1 1 0 0 1 0 0 0 1 1 0 1 0 0 1

0 1 1 0 0 0 1 1 0 1 1 0 0 0 0 1 0 1 1 1 0 1 0 0 0 1 1 0 0 1 0 1 0 1 1 0 0 1 0 0 0 0 1 0 0 0 0 0

0 1 1 1 0 1 0 0 0 1 1 0 1 1 1 1 0 0 1 0 0 0 0 0 0 0 1 1 1 0 1 0 0 0 1 1 0 1 0 0 0 0 1 1 0 0 1 0 1

ASCII Code: Patterns

Looking for patterns in number tables is one way middle school mathematics students learn about algebra. The ASCII Code table is like a function input/output table. We can focus on two columns and think of one column as the input and the other as the output.

There are two ways to look for patterns in a table like the table of ascii codes. One way is to look for a pattern going down the table. For example, going down the column labeled **Decimal** the pattern is increasing by +1 each time.

1. In the ASCII Code tables, describe a pattern you see going down the column labeled **Octal**. That is say something about how the numbers change as you go down that column. The best answer is to say exactly how to go from the number in one row to the number in the next row.

Another way to look for patterns is going across. Generally, these patterns are more difficult to describe and may require formulas and procedures. We would like to be able to completely describe the pattern from one column in the ASCII table to another. We would like to find ways of describing how to take a number from one column and calculate the number in the same row of another column.

2. Describe how to convert a **Octal** numeral to it in an **decimal** numeral.

3. Describe how to convert a **decimal** numeral to the **octal** numeral.

Teaching Patterns: 1213121412131215 . . .

On this page, write down your summary and reactions to each way the 1213 pattern was described. Write down enough information so that you could refer to this later and teach it to someone else. Which way was best for you to learn? Why? Which way would you like to teach? Why?

chanting – describing patterns
Auditory learning is a teaching and learning style in which a person learns through listening.

inches
Visual learning is a teaching and learning style in which ideas, concepts, data and other information are associated with images and techniques.

counting with fingers, standing and sitting
Kinesthetic learning is a teaching and learning style in which learning takes place by the student actually carrying out a physical activity.

Assignment: 1213121412131215 . . .

1	2	3	4
fingers	counting, place value two	counting, place value ten	1213 numbers
T	00001	1	1
I	00010	2	2
IT	00011	3	1
M	00100	4	3
MT	00101	5	1
MI	00110	6	2
MIT	00111	7	1
R	01000	8	4
RT	01001	9	1
RI	01010	10	2
RIT	01011	11	1
RM	01100	12	3
RMT	01101	13	1
RMI	01110	14	2
RMIT	01111	15	1
P	10000	16	5
PT	10001	17	1
PI	10010	18	2
PIT	10011	19	1
PM	10100	20	3
PMT	10101	21	1
PMI	10110	22	2
PMIT	10111	23	1
PR	11000	24	4
PRT	11001	25	1
PRI	11010	26	2
PRIT	11011	27	1
PRM	11100	28	3
PRMT	11101	29	1
PRMI	11110	30	2
PRMIT	11111	31	1

1. On another sheet of paper, write out the first 512 1213 numbers. Organize your work in such a way that a pattern emerges. You may use an excel worksheet if you know how. Write an explanation of this pattern.

2. Explain a pattern that you observe going down column 2 of the table on the left. Explain well enough so the reader can continue the numbers using your pattern.

3. Find pattern, or formula, that explains how to go from left to right in the table. Explain the pattern or formula. For example, explain a procedure that takes a number from column 3 and computes the corresponding number in column 2.

4. Write a careful explanation: There are 32 different ways one can hold up the five fingers of a hand.

Counting in Octaland

In Octaland the people, although similar to us in every other way, have only four fingers on each hand. Consequently, their numeration system has developed very different from our own. Here is a table that summarizes their system:

Octites count by saying	To represent this many things	The octal numeral for this number	the decimal numeral for this number
one	**I**	1	
two	**II**	2	
three	**III**	3	
four	**IIII**	4	
five	**IIII I**	5	
six	**IIII II**	6	
seven	**IIII III**	7	
oct	**IIII IIII**	10	
one-oct-one	**IIII IIII I**	11	
one-oct -two	**IIII IIII II**	12	
one-oct-three	**IIII IIII III**	13	
one-oct-four	**IIII IIII IIII**	14	
one-oct-five	**IIII IIII IIII I**	15	
one-oct-six	**IIII IIII IIII II**	16	
one-oct-seven	**IIII IIII IIII III**	17	
two-oct	**IIII IIII IIII IIII**	20	
two-oct-one	**IIII IIII IIII IIII I**	21	
two-oct-two	**IIII IIII IIII IIII II**	22	
two-oct-three	**IIII IIII IIII IIII III**	23	
two-oct-four	**IIII IIII IIII IIII IIII**	24	
two-oct-five	**IIII IIII IIII IIII IIII I**	25	
two-oct-six	**IIII IIII IIII IIII IIII II**	26	
two-oct-seven	**IIII IIII IIII IIII IIII III**	27	
three-oct	**IIII IIII IIII IIII IIII IIII**	30	
three-oct-one	**IIII IIII IIII IIII IIII IIII I**	31	
three-oct-two	**IIII IIII IIII IIII IIII IIII II**	32	
three-oct-three	**IIII IIII IIII IIII IIII IIII III**	33	
three-oct-four	**IIII IIII IIII IIII IIII IIII IIII**	34	
three-oct-five	**IIII IIII IIII IIII IIII IIII IIII I**	35	
three-oct-six	**IIII IIII IIII IIII IIII IIII IIII II**	36	
three-oct-seven	**IIII IIII IIII IIII IIII IIII IIII III**	37	
four-oct	**IIII IIII IIII IIII IIII IIII IIII IIII**	40	
four-oct-one	**IIII IIII IIII IIII IIII IIII IIII IIII I**	41	
four-oct-two	**IIII IIII IIII IIII IIII IIII IIII IIII II**	41	

Arithmetic in Octaland

All numbers on this page are octal numbers. How would you teach an Octite child to do these problems in a way that emphasizes concepts over procedures?

Adding

$$\begin{array}{r} 14 \\ +11 \\ \hline \end{array} \qquad \begin{array}{r} 27 \\ +35 \\ \hline \end{array}$$

Subtracting

$$\begin{array}{r} 55 \\ -16 \\ \hline \end{array} \qquad \begin{array}{r} 200 \\ -17 \\ \hline \end{array}$$

Multiplying

$$\begin{array}{r} 15 \\ \times\ 7 \\ \hline \end{array} \qquad \begin{array}{r} 65 \\ \times 17 \\ \hline \end{array}$$

Dividing

$$3\overline{)14} \qquad 12\overline{)604}$$

Sideways Arithmetic in Octaland

These puzzles from Octaland Sideways Arithmetic look just like the puzzles on page XX. But this time each one represents an arithmetic problem done in base 8 like the Octaland problems on page XX The digits 0, 1, 2, 3, 4, 5, 6, and 7 have been replaced by a letter of the alphabet.

These problems look the same but the arithmetic statements they encode represent different numbers than they did in decimal arithmetic. Do these same puzzles have a solution in base 8?

1.

```
  boys
+ boys
 silly
```

input:	0	1	2	3	4	5	6	7
output:		s	y		l	b	o	

2.

```
  girls
+ girls
  silly
```

input:	0	1	2	3	4	5	6	7
output:	l	g		s	r		y	i

3.

```
  arcs
+ bras
 crass
```

input:	0	1	2	3	4	5	6	7
output:	s	c		r	b			a

4.

```
 llama
- seal
  seal
```

input:	0	1	2	3	4	5	6	7
output:		l	a		ms	e		

Numbernames in Octaland

Cryptographers often use base 8 arithmetic to encode messages. This suggests another way to keep your name secret: convert it to a base 8 numeral. Cathy's numbername in base 8 is 1373525404 because

$$1x8^9 + 3x8^8 + 7x8^7 + 3x8^6 + 5x8^5 + 2x8^4 + 5x8^3 + 4x8^2 + 4 = 200190724$$

1. Convert your numbername to base 8. Explain your method.

Teaching Presentation: Crickets

1. Read MANEUVERS ON NUMBER LINES by David Page. Do all of the activities and problems – cover up the answers so you can work them out on your own first, then compare your thinking to Page's discussion of the solution.

2. What is his point: list two important ideas that Page is trying to express to teachers about teaching. What does Page mean by "simple-minded, tedious, drawn-out manner" (page -12-) what does he mean by "[. . .doing problems] as efficiently and elegantly as possible" (also page -12-).

3. You will be assigned one of the problems from More Medium Problems, that start on page -9- of the monograph, for your teaching presentation. First do the problem in a simple-minded, tedious manner as you might expect a child to do it. Second, provide a method for doing the problem more efficiently and/or elegantly. When you teach you will present both soluitons.

4. Invent a related, advanced problem that will challenge the class. You should plan to have your students do this problem in class. If you don't teach, your invented problem will be added to the list of class problems page xx.

Complete the pink and write the solutions to both problems. Hand in one copy and keep a copy for yourself. The class period after the proposal is due you will be expected to present the problem to Gail. Gail will pass you as ready or not to present to the class. Very unfortunately, there will not be time for everyone to present. For some people their presentation grade from Gail will also be their class presentation grade.

Page also says: "the challenge of inventing better methods should be shifted largely to the student. the teacher may give worthwhile hints, but whenever possible the teacher should avoid just telling the child how to do the problem." Can you teach your problem this way?

assignment	date	grade
Proposal		/20
Group Practice Presentation		/10
Class presentation		/10
Related Problem		/10

Pink Sheet: Maneuvers

Name: Date:

State two important ideas in the essay MANEUVERS ON NUMBER LINES by David Page.

1.

2.

State the problem you were assigned from More Medium Problems:

State your related, advanced probem

3. Provide solutions to both problems on separate sheets of paper

MANEUVERS ON NUMBER LINES

by

David A. Page
University of Illinois at Chicago Circle

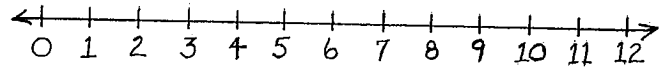
A Trip through Number Lines from
First Grade to Fifteenth Grade
for
Bright Students
or
Slow Students
or
Students In Between

Winter 1976

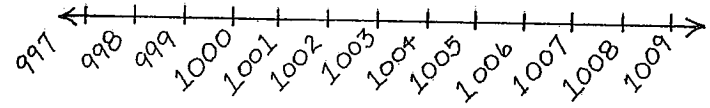
NUMBER LINES IN THE EARLY SCHOOL GRADES

Drawing a Number Line

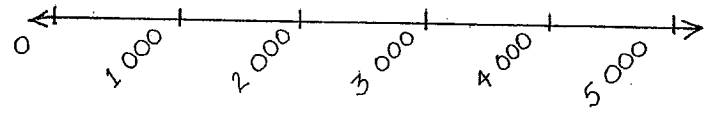
Let us consider a single number line for the young child. On blackboard, spirit duplicator, or bulletin board, draw something like this:



The line and numbers go on forever in both directions. We often draw just that part of it immediately to the right of zero. Whenever it helps us, we will draw a different piece of it



or draw it to a different scale.

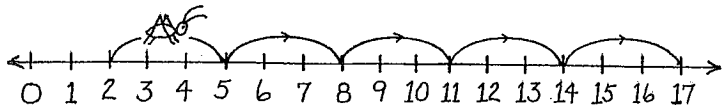


At first we shall ignore the negative numbers since schools do. However, later we will show that a number line is a great help in learning easily how to work with negative numbers.

Uniform Jumping by One Small Beast

A "plus three cricket" jumps three units to the right from wherever it is located on the line. It jumps again from wherever it lands. Suppose we start a +3 cricket from 2 on a number

line and let him jump.



Here are some questions for five and six year olds. (Most children of this age are not prepared to read these questions. But they can answer them.)

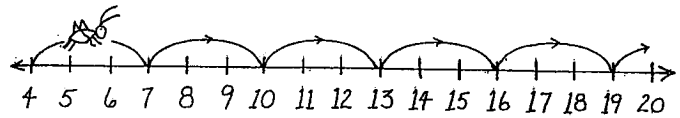
1. How many jumps does the cricket make before he jumps off of our picture of the number line? (Answer: five jumps and then he is off of our picture above.)

2. The cricket lands on some numbers (like 2 and 5) and jumps over some numbers (like 3, 4 and 6). Take a good look at the line and the cricket. Now look away. Tell whether he lands on or jumps over each of the following numbers.
   8 ? 10 ? 11 ? 13 ? 14 ? 18 ?

3. The last place we see the cricket on our line above is 17. As he goes on up the line, where does he land next? Next after that? (If a child at first needs to draw a longer line and carry out additional jumps to figure this out, fine. In time he will answer a question like this by looking at a number line drawn "in his head".)

4. Suppose we start our +3 cricket at 4. What are the next five numbers he lands on? (At first the child answers such a question by drawing a piece of the number line and carrying out the

jumps:



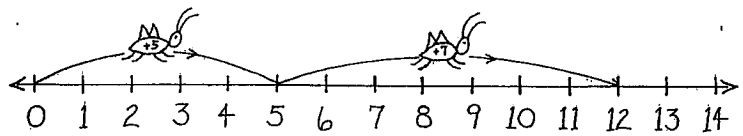
Answer: He starts at 4 and then lands on 7, 10, 13, 16, and 19 successively.)

Shortly the child learns that he can carry out this jumping in his head by counting: " 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19." But the mental imagery of the number line while counting is important.

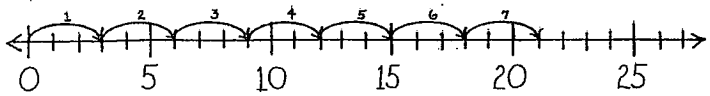
In time, when asked for the next five landing points of a cricket starting at 107, the child "just knows".

Standard Arithmetic on a Number Line

Suppose a +5 cricket makes one jump starting at zero. When he lands he is replaced by a +7 cricket which makes one more jump. Where does the second cricket land?



This, of course, is just a physical interpretation of the question 5 + 7 = ? . Suppose a +3 cricket starts at zero and makes seven jumps in succession. Where does he land?



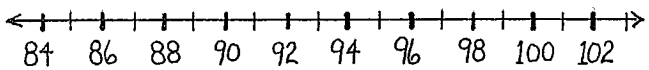
In seven jumps of +3 each he lands at 21 and we have a number line interpretation of $7 \times 3 = 21$.

Minus Crickets

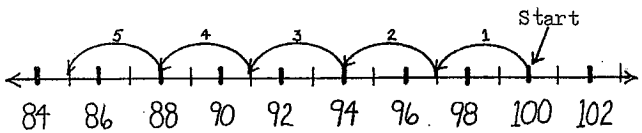
A "plus three cricket" jumps to the right -- onto bigger and bigger numbers. A "minus three cricket" jumps left on a number line -- onto smaller and smaller numbers.

Question: A " -3 cricket" starts at 100 and makes five jumps. Where does it land?

For the child who needs to (and at first almost all will need to) a detailed number line in the region around 100 should be drawn:



and then each left-going jump traced out in detail.



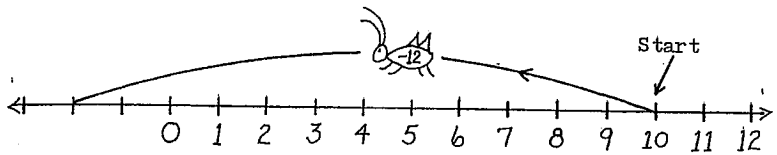
(Answer: 85)

The child has answered the question: $100 - (5 \times 3) = ?$ or, although he does not yet know it, he has even answered:

$$100 + (5 \times (-3)) = ?$$

The reader may suggest that the child is ready for: "If a ' -12 cricket' starts at 10 , where does he land?"

Even if the child has never heard of negative numbers he knows precisely where the answer to the question is located.



It can be rewarding to ask early grade students what they would like to call a number such as the number left of zero which the cricket landed on above. In the author's experience children are likely to suggest names such as:

two below (from thermometer)

002 or 02 (from fascination with zero)

two down

two "in the hole" (from playing games)

If some such home-invented terminology is used for a few weeks, there is then almost no problem telling students that, by custom, the number is usually written " -2 " and called "negative two". (Bookkeepers sometimes use red ink instead of a minus sign.)

Students in grades seven to eleven who are expected to become old timers with negative numbers in a hurry would be much better off if they had first met negative numbers on a number line in the early grades. Failing this, it should be made clear to students that there are numbers to the left of zero which eventually will get into arithmetic.

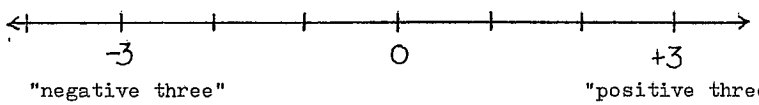
Quibbles and Modernisms

There are many matters of philosophy which an adult may bring up that seldom bother children. In fact sometimes adults become so concerned about both philosophy and propriety that the interesting mathematics disappears. Accordingly only a few such quibbles will be mentioned here.

Some people strongly believe that there is only one Real Number Line. Fine. We draw pictures and sketches to represent whatever parts of the number line we are currently concerned with. Having noted this, we will continue to say things like "draw two number lines" instead of "draw two pictures of the number line".

- - -

Some mathematics educators have made a noble attempt to call the numbers themselves, for example, "positive three" and "negative three" instead of "plus three" and "minus three".



These people save "plus" and "minus" as references to the operations of addition and subtraction. This "clarification" of language works this way.

Item	Pronunciation
-3	"negative three" (Avoid "minus three".)
$+5$	"positive five" (Avoid "plus five".)
$5-3$	"five minus three"
$5+3$	"five plus three"
$5-(-3)$	"five minus negative three"

The main difficulty with these niceties is that most professionals who work with numbers ignore them and speak of "minus four" and "negative four" interchangeably.

- - -

During the 1960's some textbooks began to use "lifted" plus and minus signs when talking about positive and negative numbers. These authors write as follows:

$^{-}5 \qquad ^{+}3 \qquad 5^{+}3 \qquad 5^{-}3$

instead of

$-5 \qquad +3 \qquad 5+3 \qquad 5-(-3)$

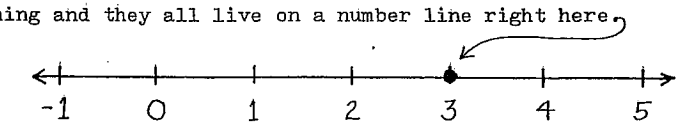
This is another reform that is in trouble because professionals don't follow it. Also it is tedious when writing by hand (which every student must do constantly while learning mathematics) to make marks so accurately that one can distinguish among:

$^{-}3 \qquad ^{-}3 \qquad -3$

In this booklet only the usual on-line plus and minus signs are employed.

- - -

Some mathematicians view the Integers, the Rational Numbers, and the Real Numbers as entirely different number systems. In this booklet the counting number 3, the integer 3, the rational number 3, and the real number 3 are all the same thing and they all live on a number line right here.



The reader who doesn't see how there could be so many different 3's is urged to smile and keep reading.

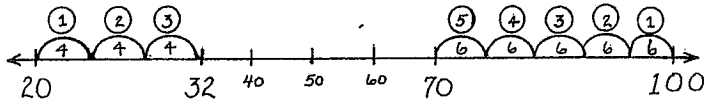
NUMBER LINES IN THE MIDDLE GRADES

A Word Problem for Fourth or Fifth Graders

There are two frogs. One frog is a +4 frog. If it is on 10, it jumps successively to 14, 18, 22, etc. The other frog is a -6 frog. If it is on 30, it jumps successively to 24, 18, 12, 6, etc.

The +4 frog starts at 20 and makes three jumps. The -6 frog starts at 100 and makes five jumps. After they have finished jumping, how far apart are the frogs?

Notice, first, that a student could (and rarely might) build a number line running from 0 to 100 and carry out each individual jump by counting along this line. Then he could count the spaces between the frogs. The trouble with this method is that it takes a long time, is a lot of work, and is so tedious as to risk "errors of boredom". (But this step by step method remains as a "backstop".). An average fourth grader more likely draws a quick sketch like:



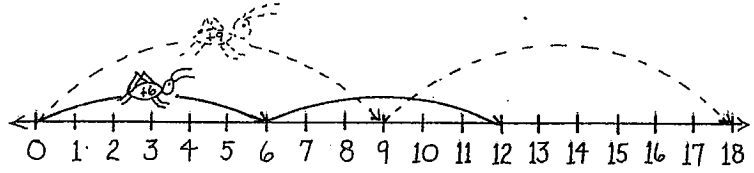
If he can do a fair amount of arithmetic, he finds 32 and 70 in the expected way. For the "distance between 32 and 70", he can merely subtract 32 from 70. If he does not know that subtraction will do the job for him, or if he doesn't know how to subtract, he can refer to the diagram he has drawn and work through the details: Between 70 and 32 there are three spaces of ten units each and one space of eight units. (Answer: The frogs finish up thirty-eight units apart.)

A variation on the preceding problem: The +4 frog starts at 20 and makes thirty-one jumps. The -6 frog starts at 100 and makes sixteen jumps. How far apart are they? (Answer: This time the frogs "cross" in the middle and end up one hundred and forty units apart.)

More Medium Problems

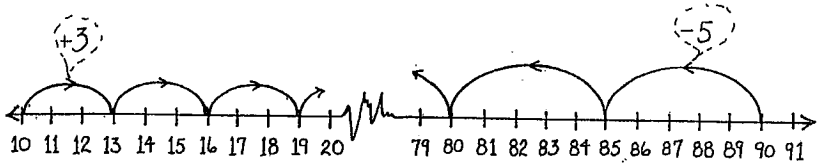
Here are a few more problems for students in the early to middle grades. They hint at the multiplicity of problems which can now be constructed.

1. A +6 cricket and a +9 cricket both start jumping at zero. They each jump lots of times. Here is a diagram showing them making their first two jumps.



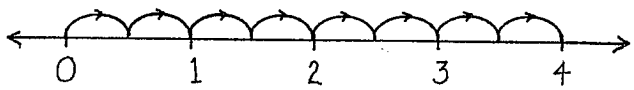
The +9 cricket gets ahead if they make their jumps together. Question: Does the +6 cricket ever come along and land on a place where the +9 cricket has already landed? What are all the places between 0 and 100 where they both land? (Answer: 18, 36, 54, 72, 90. The student has, of course, found the Common Multiples of 6 and 9 which are less than 100. The first place they both land on after zero is the Least Common Multiple. The idea can be taught with or without the terminology.)

2. A -5 cricket starts at 90 and jumps until he is near zero. A $+3$ cricket starts at 10 and jumps until he gets up past 100.



In his trip up the line does the $+3$ cricket ever land on a spot which the -5 cricket has also landed on coming down the line? Is there more than one such place? (Answers: 25, 40, 55, 70, and 85.)

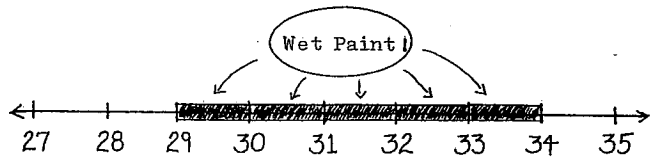
3. A $+\frac{1}{2}$ cricket jumps like this:



If it starts at zero and makes twenty-five jumps, where will it land? (Answer: $12\frac{1}{2}$. Notice that the student has done the problem: $25 \times \frac{1}{2} = ?$)

4. A $+\frac{1}{3}$ cricket starts jumping at zero. After lots of jumps it lands at 12. How many jumps did it have to make? (Answer: Since it takes three jumps to go a unit distance, it takes thirty-six jumps to get from zero to 12. The student has done the problem $12 \div \frac{1}{3} = 36$ without an appeal to magic.

5. There is wet paint on the number line starting at 29 and going on through 34.



We are going to start crickets with various jump lengths on the number line and see if they jump into the wet paint.

A $+10$ cricket starts jumping at 5 on the number line and jumps until he has crossed the painty region. Did he land in the wet paint? (Answer: No. He went to 15, 25, and then jumped clear over the painty region.)

6. Same painty region. A $+8$ cricket starts at zero and makes lots of jumps. Does he land in the paint? (Answer: Yes. He lands in the paint at 32.) Could you start him out somewhere so he would miss the paint? (Answer: Yes. You could start him lots of places where he would miss. For example, starting out on 3 would work.) Later, students can look for <u>all</u> the starting places that would avoid the paint.

7. Same painty region. A -5 cricket starts jumping at 67. Will he hit the painty region? (Answer: Yes. He will get in the paint at 32.) Could you start him on the line so he would miss the paint? (Humorous Answer: Yes. You could <u>start</u> him at 27! He would never hit the paint!)

New question: Could you start him somewhere above the painty region so he would miss the paint? (Answer: No. He will always hit. He is too short a jumper.) Some students will notice that there are some starting places which cause the cricket to land twice in the wet paint region. The author has seen an occasional fifth grade student announce that if there are any starting places which cause the cricket to land in the paint twice, then there are no places from which he can jump completely over the paint.

* * *

Notice that every problem given thus far could be solved by the student in a simple-minded, tedious, drawn-out manner. As has been pointed out, it is sometimes valuable for a student to work a problem in such complete detail. But it is more important to note that if a student knows how he would work out a problem in laborious detail, he does know what the problem is asking for. Too often a school child reads a mathematics problem and has no idea of any method he might use to solve it. He often doesn't understand what the question is asking for.

Of course, the long run goal is to do these problems as efficiently and elegantly as possible. At first look only for brief little glimpses of elegance from students. Also the challenge of inventing better methods should be shifted largely to the student. A teacher may give worthwhile hints, but whenever possible the teacher should avoid just telling the child how to do the problem. "Telling" might be fine; only the child does not stay told.

Crickets: Modeling Arithmetic with Negative Numbers

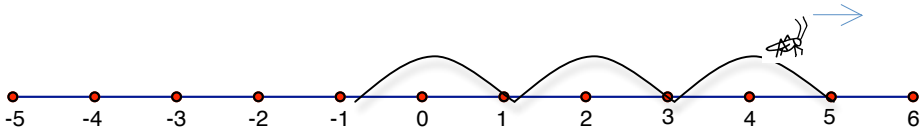
A positive cricket jumps to the right when it moves forward and jumps to the left when it moves backwards.

A negative cricket jumps to the left when it moves forward and jumps to the right when it moves backwards.

Examples:

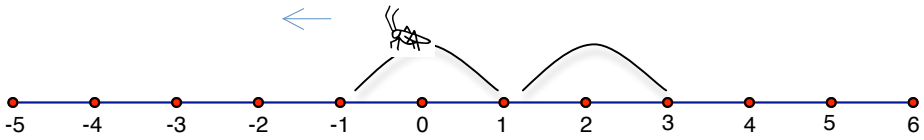
1. A +2 cricket starting at -1 jumps forwards three times and lands on 5:

-1 + 3 x 2 = 5



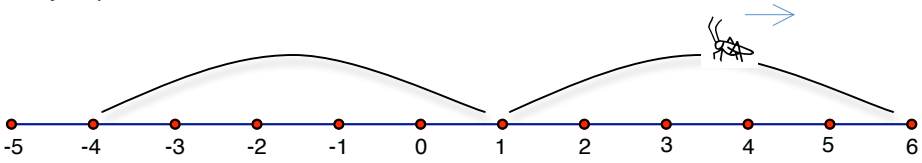
2. A -2 cricket starting at 3 jumps forwards twice and lands on -1:

3 + 2 x -2 = -1



3. A -5 cricket starting at -4 jumps backwards twice and lands on 6:

-4 - 2 x (-5) = 6



Problems: For each statement, write the corresponding arithmetic statement. Then model the statement on the number line.

4. A +5 cricket starting at 4 jumps backwards once

5. A -4 cricket starting at 3 jumps forward twice

6. A -2 cricket starting at 0 jumps backwards three times

Find the answer to each problem by showing how the cricket would move on the number line. That is, first draw the cricket jumping to see what the answer will be. Do the arithmetic to check that you got the model correct after you draw the model.

7. -4 – (-5) =

8. 3 - 2 x 4 =

9. -3 + 4 x 2 =

10. 0 - 4 x (-3) =

11. What is the difference between the expression (-4) x (-3) and the expression 0 - 4 x (-3)?

Why is a negative number times a negative number a positive number?

First we will convince ourselves that a positive number times a negative number should be a negative number. In fact we will show that 4 x (-3) = -12.

Then, confident that a positive number times a negative number is a negative number, we will convince ourselves that a negative number times a negative number is a positive number. In fact we will show that (-4) x (-3) = 12.

We will do this in such a way that you should be able to see how it works for other numbers.

Start with 4 x 3 and observe the following number pattern that we construct using multiplication facts we know about positive integers and what we know about negative numbers on a number line:

4 x (3) =	12
4 x (2) =	8
4 x (1) =	4
4 x (0) =	0
4 x (-1) =	
4 x (-2) =	
4 x (-3) =	

We start this table by filling in the multiplication facts we already know.

Then we finish by continuing the arithmetic pattern down the right hand column.

→4 x (-3) = -12

Now that we are confident that a positive number times a negative number is a positive number, we do a very similar thing to show that (-4) x (-3) = -12.

4 x (-3) =	-12
3 x (-3) =	-9
2 x (-3) =	-6
1 x (-3) =	-3
0 x (-3) =	0
(-1) x (-3) =	
(-2) x (-3) =	
(-3) x (-3) =	
(-4) x (-3) =	

We start this table by filling in the multiplication facts we learned in the first step.

Then we finish by continuing the arithmetic pattern down the right hand column.

→ (-4) x (-3) = 12 as we wanted to show.

1. Repeat this procedure with another set of numbers. For example, show that (-7) x (-5) = 35

Crickets and Arithmetic Sequences

Definition: An *Arithmetic Sequence* is a sequence created with a starting with a number. and a *difference* number. Each subsequent entry after the starting numbe is obtained from the previous entry by adding the difference number.

Example: A +3 cricket that starts at 2, hops out an arithmetic sequence:

2, 5, 8, 11, 14, 17, . . .

The starting number is 2; the difference number is the same as the cricket number, 3. A formula for the *n*th number in the sequence is given by $2+3\cdot n$. When $n = 0$ the cricket is on 2, the starting number. When $n = 1$ the cricket is on 5, when $n = 2$ the cricket is on 5, etc.

The numbers in an arithmetic sequence can be decreasing. A -5 cricket starting on 18 jumps:

18, 13, 8, 3, -2, -7, -12, . . .

A formula for this arithmetic sequence would be 18 - 5n, the $(n-1)^{th}$ number on the list or, for the cricket, $18 - 5n$ is where the cricket is after the n^{th} jump

Arithmetic sequences are often given in input-output tables where the input is the *term number*. In fact, we can think of a sequence as a function whose domain is the set of whole numbers. In general, the range of a sequence can be any set of numbers. In this course, the range will be integers.

input:	0	1	2	3	4	5	6	7	8	9	...	n
output:	18	13	8	3	-2	-7	-12	-17	-22	-27		18 - 5n

Definition: An *Arithmetic Progression* is an arithmetic sequence in both directions. This is like a function whose domain is all the integers.

Example: Consider where the +3 cricket was before she got to the starting point. We could still use the formula, $2+3\cdot n$, but use negative values of n as representing time *before* the start. The entire progression may be written, in part by

. . . -13, -10, -7, -4, -1, 2, 5, 8, 11, 14, 17, . . .

1. Write out the arithmetic sequence for a -4 cricket starting at 15. Write a formula for this arithmetic sequence.

2. Write a formula for an arithmetic progression with a constant difference of +7 that has the value 17 when $n = 2$.

Crickets: Writing formulas and Equations

1. If a +7 cricket starts on -9 write a formula for where he lands on his n^{th} jump.

2. How many jumps does it take for a -17 cricket starting at 103 to land on 2? Write an equation to solve to find the answer.

3. What kind of +cricket made these jumps? Fill in the rest of the landing numbers.

6 82

Try another one:

-113 19

Explain a procedure for doing this kind of problem. Write a formula for each cricket that tells what numbers it lands on. Be sure to say what your variable means in terms of where the cricket started.

Crickets: Other Concepts

Include here the examples from the teaching projects.
We will see this kind of problem again when we study the division algorithm.

1. What is the smallest positive number that a +8 cricket would start on in order to eventually land on 100? How many jumps would it take to get there? Solve on a number line. Write an arithmetic statement that shows the answer.

Crickets: Other Problems

For each problem:

- Solve in a simple-minded, tedious manner.
- Show a more efficient way to solve the problem.
- Write a cricket problem that does the same mathematics.

2. The radio station gave away a discount coupon to every fifth caller and a CD to every sixth caller. Every twentieth caller received free concert tickets. Which caller was first to get both a coupon and a concert ticket? Which caller was first to get all three prizes? If there were 150 callers, how many of each prize did they give away?

```
20=lcm(5,20),60=lcm(5,6,60),150/5=30 discount tickets,150/6=25 CD,
150/20=7 R 10 so 7 concert tickets
```

3. Larry and Mary bought a special 360-day joint membership to a tennis cub, Larry will use the club every other day, and Mary will use the club every third day. They both use the club on the first day. How many days will neither person use the club in the 360-days?

```
Groups of 6containing 2 non-days each = 2x360/6 = 120 days
```

1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18
19	20	21	22	23	24	25	26	27	28	29	30	31	32	33	34	35	36
37	38	39	40	41	42	43	44	45	46	47	48	49	50	51	52	53	54
55	56	57	58	59	60	61	62	63	64	65	66	67	68	69	70	71	72
73	74	75	76	77	78	79	80	81	82	83	84	85	86	87	88	89	90
91	92	93	94	95	96	97	98	99	100	101	102	103	104	105	106	107	108
109	110	111	112	113	114	115	116	117	118	119	120	121	122	123	124	125	126
127	128	129	130	131	132	133	134	135	136	137	138	139	140	141	142	143	144
145	146	147	148	149	150	151	152	153	154	155	156	157	158	159	160	161	162
163	164	165	166	167	168	169	170	171	172	173	174	175	176	177	178	179	180
181	182	183	184	185	186	187	188	189	190	191	192	193	194	195	196	197	198
199	200	201	202	203	204	205	206	207	208	209	210	211	212	213	214	215	216
217	218	219	220	221	222	223	224	225	226	227	228	229	230	231	232	233	234
235	236	237	238	239	240	241	242	243	244	245	246	247	248	249	250	251	252
253	254	255	256	257	258	259	260	261	262	263	264	265	266	267	268	269	270
271	272	273	274	275	276	277	278	279	280	281	282	283	284	285	286	287	288
289	290	291	292	293	294	295	296	297	298	299	300	301	302	303	304	305	306
307	308	309	310	311	312	313	314	315	316	317	318	319	320	321	322	323	324
325	326	327	328	329	330	331	332	333	334	335	336	337	338	339	340	341	342
343	344	345	346	347	348	349	350	351	352	353	354	355	356	357	358	359	360

Crickets on Spirals

Finding remainders when dividing by 26 on the Mod Spiral

On the Mod 26 Spiral, will a +5 cricket eventually land on every spoke? Will a +6 cricket eventually land in every spoke? Can you determine which crickets, if any, will eventually land on every spoke?

Some Definitions and previous notions

The counting numbers or **natural numbers** are 1, 2, 3, 4, 5, 6. . . .

The **whole numbers** are the counting numbers with zero added: 0, 1, 2, 3, 4, 5, 6. . . .

The **integers** are the counting numbers and zero and negative numbers.

. . . -5, -4, -3, -2, -1, 0, 1, 2, 3, 4, 5, 6 . . .

The counting numbers are also called the positive integers. The whole numbers are also called the non-negative integers.

1. For each of the following interpretations, select sample numbers for the variables and draw a picture to illustrate the concept.

Meaning of addition
$a + b$ is the number of objects when combining a group of a objects with a group of b objects.

Meaning of multiplication
$a \cdot b$ is the number of objects in a groups with b objects in each group.

Meaning of subtraction
$c - b$ is the number of objects when b objects are taken away from c objects.

Meaning of division We think of $a \div d$ in two ways

$a \div d$ is *how many groups* can be made of a objects, putting d objects in each group.

OR

$a \div d$ is *how many objects in each group* if a objects are grouped into d groups.

With these models or similar ones children learn their addition, subtraction, multiplication and division facts. They also learn about all the rules of arithmetic that are made formal into rules for algebra when they get to algebra. See next page.

Basic Rules of Arithmetic

There are two basic operations on real numbers: addition and multiplication. We know that we can add any two real numbers and that the answer is unique. We know that we can multiply any two real numbers and that the answer is unique.

Basic rules of addition:

Commutative Property of Addition:	For any numbers a and b, $a+b= b+a$
Associative Property of Addition:	For any numbers a, b and c, $a+(b+c) = (a+b)+c$
There is an Additive Identity:	There is a unique number, 0, such that, for any number a, $a + 0 = a$
Additive Inverses Exist:	For any number a, there is a unique number, denoted by ^{-}a such that $a + (-a) = 0$

Basic rules of multiplication:

Commutative Property of Multiplication:	For any numbers a and b, $a \cdot b=b \cdot a$
Associative Property of Multiplication:	For any numbers a, b and c, $a \cdot (b \cdot c) = (a \cdot b) \cdot c$
There is a Multiplicative Identity:	There is a unique number, 1, such that, for any number a, $a \cdot 1 = a$
Multiplicative Inverses Exist:	For any *nonzero* number a, there is an unique number, noted by a^{-1}, such that $a \cdot a^{-1} = 1$

The rule that relates multiplication and addition:

The Distributive Property:	For any numbers, b and c, $a \cdot (b + c) = a \cdot b + a \cdot c$

From these rules we have a way to think about the meaning of subtraction and the meaning of division that is different from what may be presented in elementary school:

Meaning of subtraction:
Subtracting b from a is like adding the additive inverse of b *to* a.

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

Note that this way of thinking about subtraction gives meaning to negative numbers.

Meaning of division:
Dividing a by b from is like multiplying a by the multiplicative inverse of b.
$a \div d$ is the unique number that when multiplied by d you get a.

$a \div b = a \cdot (b^{-1})$

Note that this way of thinking about division gives meaning to fractions:

$$\frac{a}{b} = a \cdot (b^{-1}) \quad a$$

Use the Basic Rules of Arithmetic and these new meanings for subtraction and division to show that these statements are true.

1. For any numbers a, b, and c, $(b + c) \cdot a = b \cdot a + c \cdot a$

2. For any numbers a, b, and c, $a \cdot (b - c) = a \cdot b - a \cdot c$

3. For any numbers a and c, $a \cdot c \cdot a^{-1} \cdot c^{-1} = 1$ and so $(a \cdot c)^{-1} = a^{-1} \cdot c^{-1}$

4. For any numbers a, b, c and d, $\frac{a}{b} + \frac{c}{d} = \frac{a \cdot d + c \cdot d}{b \cdot d}$

More basic rules for Algebra

Rules about Equations

The Basic moves for Solving an Equation:
If you start with an equation and add the same number to each side, you do not change the solutions of that equation.

If you start with an equation and add the same number to each side, you do not change the solutions of that equation.

If you change any expression in an equation, following the rules of Algebra, you do not change the solutions of that equation.

You can also subtract the same number from both sides of an equation. You can divide both sides of an equation by the same number and not change the solutions. Why do you think these rules are not on the list of basic moves? (Quote: CMP page 145)

Explain which rule was used to while solving this linear equation:

$3x + 7 = 22$	given equation to solve
$(3x + 7) + -7 = 22 + -7$	adding same number to both sides
$3x + (7 + -7) = 15$	associative addition rule, arithmetic fact
$3x + 0 = 15$	additive inverses
$3x = 15$	additive identity
$3^{-1} \cdot (3x) = 3^{-1} \cdot 15$	multiplying both sides by same number
$(3^{-1} \cdot 3)x = 5$	Associative multiplication rule, arithmetic fact
$1 \cdot x = 5$	multiplicative inverses
$x = 5$	multiplicative identity

Finally, we need to check to see if the answer is correct;

$$3 \cdot 5 + 7 = 15 + 7 = 22 \checkmark$$

1. Solve the following equation step by step. Explain which rules you are using as you go.

$8 - x = 2x + 6$

Identifying Identities

An identity for real numbers is an equation involving mathematical expressions that holds true when any real numbers are substituted for the variables. For example, $a + b = b + a$, is an identity that because commutative rule of addition holds for all real numbers.

On the other hand, $a + b = a$, is not an identity because it is only true if $b = 0$.

Which of the following are identities? For each identity, using the properties of arithmetic, give a convincing argument that the equation is always true. For each equation that is not an identity, give examples when the equation is false.

1. $\left(a + b\right)^2 = a^2 + b^2$

2. $(2ab)^2 = 4(ab)^2$

3. $2\left(a \cdot b\right) = \left(2a \cdot 2b\right)$

4. $\frac{a}{b} + \frac{c}{d} = \frac{a + c}{b + d}$

5. $\left(a + b\right)^2 = a^2 + 2a \cdot b + b^2$

6. $4\left(a \cdot b\right) = \left(2a \cdot 2b\right)$

7. $(a + b) \cdot (c + d) = ac + ad + bc + bd$

The Division Algorithm

Division does not always have a whole number solution. In number theory we are not so often interested in the remainder as a fractional part of the divisor, but in keeping track of how many objects are left over. This is division with remainder. Here are some examples:

- Gramma wants to give as many children as she can 25¢. She has a jar with 531 pennies in it to give. How many children get 25¢ and how many pennies are left over?

- What is the smallest positive number that a +23 cricket would start on in order to eventually land on 177? How many jumps would it take to get there?

This is the rule we are using when we divide and get a whole number remainder.

> **The Division Algorithm** Given two integers, m and $n \neq 0$, there exist *unique* integers q and r, with
>
> $$m = q \cdot n + r, \text{ and } 0 \leq r < n$$

If both n and m are positive, we can find q and r by repeatedly subtracting n from m. Stop the last time you are able to subtract without going less than zero: q is the number of times you subtracted n and r is the amount left over. This is shown for our example at the right. Of course, we know how to compute q and r by dividing and then finding the whole number remainder.

177		
−23	1	
154		
−23	2	
131		
−23	3	
108		
−23	4	
85		
−23	5	
62		
−23	6	
39		
−23	7	← q
16		← r

Negative numbers: If either n or m or both are negative, we can still find q and r. We may have to add instead of subtract and we may have to go past zero to ensure that r is *positive*, as required.

- What is the smallest positive number that a −23 cricket would start on in order to eventually land on −177? How many jumps would it take to get there?

For any positive or negative values for m and n, crickets provide a model. Think of m as a starting place and n (whether positive or negative) as the cricket. To find q and r, the cricket takes off towards 0 – going forwards or *backwards* as needed – and stops at the positive landing spot closest to 0. The number of jumps is q and the landing spot is r.

Examples: If $m = 60$, $n = 7$, then $q = 8$ and $r = 4$. $60 = 8 \cdot (7) + 4$
If $m = -60$, $n = 7$, then $q = -9$ and $r = 3$. $-60 = -9 \cdot 7 + 3$
If $m = 60$, $n = -7$, then $q = -8$ and $r = 4$. $60 = -8 \cdot (-7) + 4$
If $m = -60$, $n = -7$, then $q = 9$ and $r = 3$. , $-60 = 9 \cdot (-7) + 3$

Problems: Find q and r for the given values of m and n. Explain with an arithmetic statement.

a. $m = 124$, $n = 4$

b. $m = -100$, $n = 23$

c. $m = 104$, $n = -7$

d. $m = -215$, $n = -10$

Special Case: $r = 0$

In the special case when $r = 0$, we say that n **divides** m. In other words, n **divides** m if there exists an *unique* number q such that

$$m = q \cdot n$$

Note that either m or n or both may be negative.

A word about uniqueness: Both the division algorithm and the special case guarantee an *unique* number. This means that no other number will do the same thing. It may seem obvious to you that there is only one number that, when multiplied *n,* gives *m,* but it is important mathematically that multipliers be unique. If there were two different numbers I could multiply by n to get *m,* then there would not be any division, because I would not know which of the possible multipliers to choose. This is why 0 does not divide 0. In fact $0 = q \cdot 0$ for any value of q. Since q is not unique, 0 doesn't divide 0.

Notations: For *n, m* integers, "***n* divides *m***" is sometimes written: $n \mid m$

NOTE: $n \mid m$ means that $\frac{m}{n} = q$, where n is an integer. We also write: $m \div n = q$ and $n\overline{)m}^{\,q}$.

In more familiar language, we also say that n is a *factor* of m or that m is a *multiple* of *n.*

Practice: Which of the following statements are true? Which are false?

1. 24 | 4
2. 4 | 24
3. 7 | 48
4. For any two integers p and n, $p \mid p \cdot n$
5. 21 is a factor of 7.
6. 21 is a multiple of 7.
7. Any non-zero number divides 0.
8. Zero is a multiple of any number.
9. Zero divides any number.
10. There are four numbers that divide 3.

Finding remainders using a calculator

11. Describe the method you use to find the whole number remainder using a calculator.

Why does a negative × a negative = a positive?

(including how to explain it to your younger brother or sister)

For too many people, mathematics stopped making sense somewhere along the way. Either slowly or dramatically, they gave up on the field as hopelessly baffling and difficult, and they grew up to be adults who—confident that others share their experience—nonchalantly announce, "Math was just not for me" or "I was never good at it."

Usually the process is gradual, but for Ruth McNeill, the turning point was clearly defined. In an article in the Journal of Mathematical Behavior, *she described how it happened:*[1]

> What did me in was the idea that a negative number times a negative number comes out to a positive number. This seemed (and still seems) inherently unlikely—counterintuitive, as mathematicians say. I wrestled with the idea for what I imagine to be several weeks, trying to get a sensible explanation from my teacher, my classmates, my parents, anybody. Whatever explanations they offered could not overcome my strong sense that multiplying intensifies something, and thus two negative numbers multiplied together should properly produce a *very* negative result. I have since been offered a moderately convincing explanation that features a film of a swimming pool being drained that gets run backwards through the projector. At the time, however, nothing convinced me. The most commonsense of all school subjects had abandoned common sense; I was indignant and baffled.
>
> Meanwhile, the curriculum kept rolling on, and I could see that I couldn't stay behind, stuck on negative times negative. I would have to pay attention to the next topic, and the only practical course open to me was to pretend to agree that negative times negative equals positive. The book and the teacher and the general consensus of the algebra survivors of society were clearly more powerful than I was. I capitulated. I did the rest of algebra, and geometry, and trigonometry; I did them in the advanced sections, and I often had that nice sense of "aha!" when I could suddenly see how a proof was going to come out. Underneath, however, a kind of resentment and betrayal lurked, and I was not surprised or dismayed by any further foolishness my math teachers had up their sleeves.... Intellectually, I was disengaged, and when math was no longer required, I took German instead.

Happily, Ruth McNeill's story doesn't end there. Thanks to some friendships she formed in college, her interest in math was rekindled. For most of our students, there is no rekindling. This is a tragedy, both for our students and for our country. Part of the reason students give up on math can be attributed to the poor quality of most of the math textbooks used in the United States. Many texts are written with the premise that if they end a problem with the words, "Explain your answer," they are engendering "understanding." However, because these texts do not give students what they would need to enable them to "explain," the books only add to students' mystification and frustration.

Here is an example of how a widely acclaimed contemporary math series handles the topic that baffled Ruth McNeill: After a short set of problems dealing with patterns in multiplication of integers from 5 to 0 times (–4), the student is asked to continue the pattern to predict what (–1)(–4) is and then to give the next four equations in this pattern. There are then four problems, one of them being the product of two negative numbers. In the follow-up problems given next, there are four problems dealing with negative numbers, the last of which is the only one treating multiplication of negative numbers. This is how it reads: "When you add two negative numbers, you get a negative result. Is the same true when you multiply two negative numbers? Explain."

The suggested answer to the "explain" part is: "The product of two negative numbers is a positive." This is not an explanation, but a claim that the stated answer is correct.

Simply asking students to explain something isn't sufficient. They need to be taught enough so that they can explain. And they need to learn what an explanation is and when a statement is not an explanation.

The excerpt that follows is taken from a serious but lively volume entitled Algebra *by I.M.Gelfand and A. Shen, which was originally written to be used in a correspondence school that Gelfand had established. Contrast the inadequate treatment of the multiplication of negative numbers described above to the way Gelfand and Shen handle the topic.*[2] *Although their presentation would need to be fleshed out more if it's being presented to students for the first time, it provides us with a much better model for what "explain" might entail, offering as it does both an accessible explanation and a formal proof.*

—Richard Askey

The multiplication of negative numbers

To find how much three times five is, you add three numbers equal to five:

$$5 + 5 + 5 = 15.$$

The same explanation may be used for the product $1 \cdot 5$ if we agree that a sum having only one term is equal to this term. But it is evidently not applicable to the product $0 \cdot 5$ or $(-3) \cdot 5$: Can you imagine a sum with a zero or with minus three terms?

However, we may exchange the factors:

$$5 \cdot 0 = 0 + 0 + 0 + 0 + 0 = 0,$$

$$5 \cdot (-3) = (-3) + (-3) + (-3) + (-3) + (-3) = -15.$$

So if we want the product to be independent of the order of factors (as it was for positive numbers) we must agree that

$$0 \cdot 5 = 0, \quad (-3) \cdot 5 = -15.$$

Now let us consider the product (–3) · (–5). Is it equal to –15 or to +15? Both answers may have advocates. From one point of view, even one negative factor makes the product negative—so if both factors are negative the product has a very strong reason to be negative. From the other point of view, in the table

3 · 5 = +15	3 · (–5) = –15
(–3) · 5 = –15	(–3) · (–5) = ?

we already have two minuses and only one plus; so the "equal opportunities" policy requires one more plus. So what?

Of course, these "arguments" are not convincing to you. School education says very definitely that minus times minus is plus. But imagine that your small brother or sister asks you, "Why?" (Is it a caprice of the teacher, a law adopted by Congress, or a theorem that can be proved?) You may try to answer this question using the following example:

3 · 5 = 15	Getting five dollars three times is getting fifteen dollars.
3 · (–5) = –15	Paying a five-dollar penalty three times is a fifteen-dollar penalty.
(–3) · 5 = –15	Not getting five dollars three times is not getting fifteen dollars.
(–3) · (–5) = 15	Not paying a five-dollar penalty three times is getting fifteen dollars.

Another explanation. Let us write the numbers

1, 2, 3, 4, 5,...

and the same numbers multiplied by three:

3, 6, 9, 12, 15,...

Each number is bigger than the preceding one by three. Let us write the same numbers in the reverse order (starting, for example, with 5 and 15):

5, 4, 3, 2, 1
15, 12, 9, 6, 3

Now let us continue both sequences:

5, 4, 3, 2, 1, 0, –1, –2, –3, –4, –5,...
15, 12, 9, 6, 3, 0, –3, –6, –9, –12, –15,...

Here –15 is under –5, so 3 · (–5) = –15; plus times minus is minus.

Now repeat the same procedure multiplying 1, 2, 3, 4, 5,... by –3 (we know already that plus times minus is minus):

1, 2, 3, 4, 5
–3,–6, –9, –12, –15

Each number is three units less than the preceding one. Now write the same numbers in the reverse order:

5, 4, 3, 2, 1
–15, –12, –9, –6, –3

and continue:

5, 4, 3, 2, 1, 0, –1, –2, –3, –4, –5,...
–15,–12, –9, –6, –3, 0, 3, 6, 9, 12, 15,...

Now 15 is under –5; therefore (–3) · (–5) = 15.

Probably this argument would be convincing for your younger brother or sister. But you have the right to ask: So what? Is it possible to *prove* that (–3) · (–5) = 15?

Let us tell the whole truth now. Yes, it is possible to prove that (–3) · (–5) *must be* 15 *if* we want the usual properties of addition, subtraction, and multiplication that are true for positive numbers to remain true for any integers (including negative ones).

Here is the outline of this proof: Let us prove first that 3 · (–5) = –15. What is –15? It is a number opposite to 15, that is, a number that produces zero when added to 15. So we must prove that

3 · (–5) + 15 = 0.

Indeed,

3 · (–5) + 15 = 3 · (–5) + 3 · 5 = 3 · (–5 + 5) = 3 · 0 = 0.

(When taking 3 out of the parentheses we use the law $ab + ac = a(b + c)$ for $a = 3$, $b = –5$, $c = 5$; we assume that it is true for all numbers, including negative ones.) So 3 · (–5) = –15. (The careful reader will ask why 3 · 0 = 0. To tell you the truth, this step of the proof is omitted—as well as the whole discussion of what zero is.)

Now we are ready to prove that (–3) · (–5) = 15. Let us start with

(–3) + 3 = 0

and multiply both sides of this equality by –5:

((–3) + 3) · (–5) = 0 · (–5) = 0.

Now removing the parentheses in the left-hand side we get

(–3) · (–5) + 3 · (–5) = 0,

that is, (–3) · (–5) + (–15) = 0. Therefore, the number (–3) · (–5) is opposite to –15, that is, is equal to 15. (This argument also has gaps. We should prove first that 0 · (–5) = 0 and that there is only one number opposite to –15.) □

[1] Ruth McNeill, "A Reflection on When I Loved Math and How I Stopped." *Journal of Mathematical Behavior*, vol. 7 (1988) pp. 45-50.

[2] *Algebra* by I. M. Gelfand and A. Shen. Birkhauser Boston (1995, Second Printing): Cambridge, Mass. © 1993 by I. M. Gelfand. Reprinted with permission.

Substitution Tables for Encrypting and Decrypting

Cipher tables for can be written in different ways. In this table for a substitution cipher the plaintext is alphabetized.

Table I:

a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z
F	B	A	V	S	M	Q	C	T	X	U	K	W	P	Y	Z	G	L	E	O	N	J	D	H	R	I

Use **Table I** to encrypt and decrypt these messages:

Encrypt										Decrypt						
c	i	p	h	e	r					t	a	b	l	e	s	
A	T	Z	C	S	L					O	F	B	K	S	E	

In this table for the same substitution cipher the CIPHERTEXT is alphabetized.

Table II

c	b	h	w	s	a	q	x	z	v	l	r	f	u	t	n	g	y	e	i	k	d	m	j	o	p
A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z

Use **Table II** to encrypt and decrypt these messages:

Encrypt										Decrypt						
a	r	e		f	u	n				t	o		u	s	e	
F	L	S		M	N	P				O	Y		N	E	S	

It doesn't make any difference how the cipher is listed. In both cases that plaintext "a" goes with ciphertext "F", plaintext "b" goes with "B", and so on. In both cases that ciphertext "A" goes with plaintext "c", ciphertext "B" goes with plaintext "b", and so on. However, it may make a difference for some people in how easy it is encrypt or decrypt messages.

---

1. Check that all plaintext-CIPHERTEXT pairs are the same for both tables on this page.

2. Use both tables to encrypt your name. Use both tables to decrypt: R Y N L P F W S

_____ _____

3. Which type of table do you think is easier to use?

Counting: How many Ciphers Tables are there?

403,291,461,126,605,635,584,000,000

Wow. This is a big, big number. Let's think about it?

Problem: How many different cipher tables can I make using an alphabet of the twenty-six letters?

Remember: I want to make "good" ciphers. So I don't want any two different plaintext letters to encrypt to the same ciphertext letter. And I don't want any two different ciphertext letters to decrypt to the same plaintext letter. That means that each row of the cipher table must contain all twenty-six letters.

Like many problems it helps to start with simpler problems. In this case, let's consider shorter alphabets. Looking for patterns and organizing your work into a table is also a good idea.

Do simpler problems:

How many different cipher tables can I make using an alphabet of just two letters?

How many different cipher tables can I make using an alphabet of three letters?

How many different cipher tables can I make using an alphabet of four letters?

Table:

number of letters in the alphabet	number of possible cipher tables	
2	2	2·1
3	6	3·2·1
4	24	4·3·2·1
5	120	5·4·3·2·1
6	720	6·5·4·3·2·1
7		
8		
9		
. . .		
26	26!	
formula: n	n!	

What is the pattern? Can you write a formula for the number of different cipher table for an alphabet with n letters.

Teaching Big Numbers

It can help students understand exactly how truly large numbers can get to make comparisons to quantities and measurements they may understand

Consider the following questions about the number 403,291,461,126,605,635,584,000,000. Do some research to find answers to these questions. Think of some more questions that might be interesting and help put the size of this number into context.

If this number were a number of seconds, how many years would it represent?

If this number were a number of miles how many round trips to the moon would it represent?

If this number were a number of living cells, how many human beings would it represent?

Patterns in Substitution Ciphers

The problem with using general substitution ciphers is that you must tell any potential decrypter the whole cipher table. However, if you can agree on a pattern in advance, the decrypter can generate the cipher as needed. Keyword Ciphers are an example. As are Caesar Ciphers

One this page you can try your hand at making your own pattern.

1. Use this table to make your own substitution cipher. Use a pattern. Do not use Keyword or Caesar cipher patterns.

Name of your cipher:_____

a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z

Describe your pattern:

Sometimes it is easier to describe patterns with numbers.

2. Enter your cipher here with both plaintext and CIPHER TEXT coded with Crypto Club letter-to-number code. What number patterns do you see?

0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25

Describe your pattern using numbers:

3. Encrypt your name using your cipher. Describe your pattern to the class and see if they can guess your name.

Your name plaintext																	
Your name encrypted																	

Cryptography in Spanish: Frequency Analysis

After discussion of crack Caesar.

Try cracking these Spanish quotes. The original plaintext is Spanish. Each was encrypted using a different Caesar Shift.

V Z N J W T Y W F G F O F W J S Q T V Z J F R N R J

L Z X Y F , D S T U F W F W M F X Y F H T S X J L Z N W Q T ,

F Z S V Z J R J Y J S L F V Z J N W F Q F Q Z S F .

- - L Z N Q Q J W R T M F W T (F X Y W T S F Z Y F)

key=5, most common: F(a) 17.5%

Y Z P D E F O T Z A Z C D L M P C X L D , D T Y Z A Z C

T R Y Z C L C X P Y Z D - - D Z C U F L Y L T Y D O P W L

N C F K .

key=11, most common Z (o) 13.5%

P F E F G Z E K D Z J J L V F J G Z E K D Z I V R C Z U R U G F I H

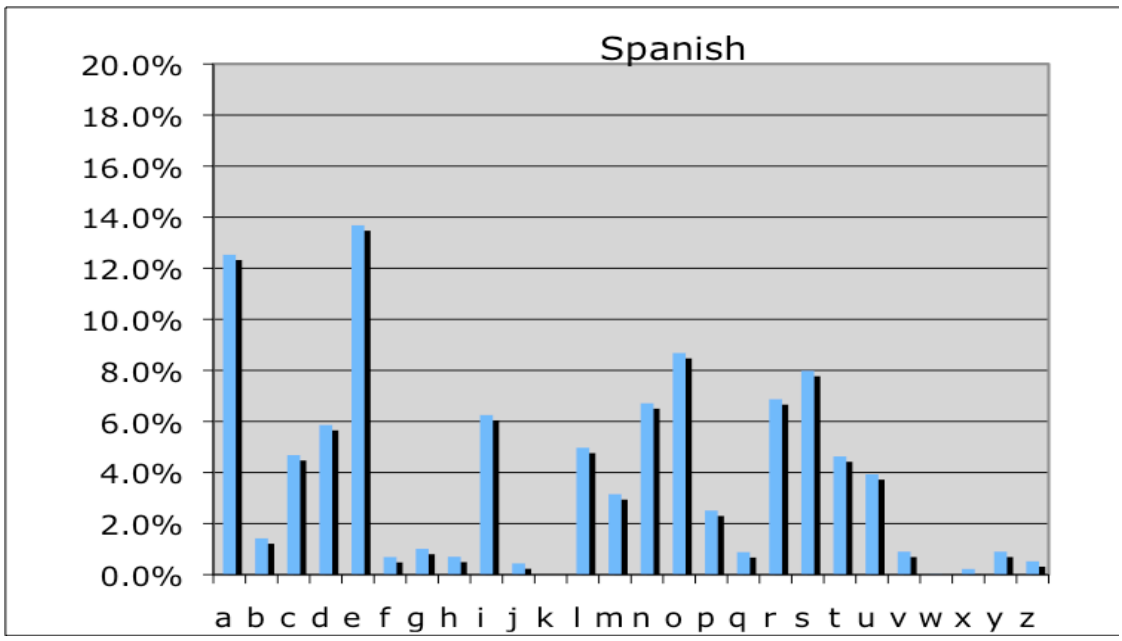
L V V I R C F E Z T F H L V K V E R F G F I H L V V I R C F E Z T F

H L V T F E F T R W I Z U R B R Y C F

key=17, most common: F(o) 15%

Computing Frequencies: Spanish

Use the same tally sheets and percentage tables.



Guess the Keyword

There is no apparent reason why one number is prime and another not. To the contrary, upon looking at these numbers one has the feeling of being in the presence of one of the inexplicable secrets of creation. -- D. Zagier

G Y V D V Z F E A Q B B Q D V E G D V Q F A E K Y N A E V

E H M S V D Z F B D Z M V Q E U Q E A G Y V D E A G . G A

G Y V T A E G D Q D N , H B A E I A A R Z E X Q G G Y V F V

E H M S V D F A E V Y Q F G Y V W V V I Z E X A W S V Z E X

Z E G Y V B D V F V E T V A W A E V A W G Y V

Z E V L B I Z T Q S I V F V T D V G F A W T D V Q G Z A E . - -

U . O Q X Z V D

V	16.6
E	11.4
A	9.7
G	8.0
D	7.4
Q	6.3
Z	6.3
F	5.1
Y	5.1
B	3.4
T	2.9
W	2.9
I	2.3
S	2.3
X	2.3
H	1.7
M	1.7
N	1.1
U	1.1
K	0.6
L	0.6
O	0.6
R	0.6
C	0.0
J	0.0
P	0.0

keyword=PRIME, keyletter=j

The problem of distinguishing prime numbers from composite numbers and of resolving the latter into their prime factors is known to be one of the most important and useful in arithmetic. -- C.F. Gauss

G M Z A D Y V T Z H Y N X B F G B O U I B F M B O U A D B H Z

O I H V Z D F N D Y H W Y H A Y F B G Z O I H V Z D F S O X Y N

D Z F Y T J B O U G M Z T S G G Z D B O G Y G M Z B D A D B H Z

N S W G Y D F B F R O Y K O G Y V Z Y O Z Y N G M Z H Y F G

B H A Y D G S O G S O X I F Z N I T B O S D B G M H Z G B W.

-- W.N. USIFF

G	9.9
Z	9.9
B	9.3
Y	9.3
O	8.0
D	7.4
F	7.4
H	6.2
N	4.3
S	4.3
I	3.7
M	3.7
A	3.1
T	2.5
U	2.5
V	2.5
W	2.5
X	1.9
J	0.6
K	0.6
R	0.6
C	0.0
E	0.0
L	0.0
P	0.0
Q	0.0

Keyword=NUMBERTHEORY keyletter=f

Factors: Definitions and Examples

Definitions: A *factor* of a number is one of two or more integers that divides the number without remainder. Another word for factor is *divisor*. We say that one number *divides* another number if the first is a divisor of the second.

Examples: 5 is a factor of 15 because 15 = 5 X 3.

We also say, "5 divides 15" and 5 is a divisor of 15.
6 is not a factor (or divisor) of 15 because 15 ÷ 6 = 2 R 3.

Although we are often interested in finding positive factors, the definition allows for negative numbers:

Examples: -5 is a factor of 15. 3 is a factor of -15. -5 is a factor of -15.

Definition: A *multiple* of an integer is the result of multiplying that integer by any other integer. This includes multiplying by 0 and negative numbers.

Examples: 15, 30, and 60 are multiples of 15. So are -15, -30, and 0.

Definition: *Factoring* a number means to find all positive factors.

1. The bookstore marked down some notepads from $2.00 but still kept the price over $1.00. It sold all of them. The total amount of money from the sale of the pads was $31.45. How many notepads were sold?

2. Mary saw a cricket land on 36 and later on 102. Which crickets could do this? List them all.

3. How often will a +3 cricket starting on 0 land on a multiple of 7? How often will a +3 cricket starting on 2 land on a multiple of 7? How often will a +3 cricket starting on 9 land on a multiple of 7?

GCD and problems

Definition: The *greatest common divisor or* gcd of two or more non-zero numbers is the greatest positive integer that divides all of the numbers. The greatest common divisor of two non-zero integers *A* and *B* is abbreviated by gcd(*A, B*). Sometimes in elementary school it is called the *greatest common factor*.

There are many ways to compute the gcd of two or more numbers:

1 -- List all of the factors of each number. Circle any factor they all have in common. Find the largest of the circled numbers. Find the gcd (168, 154)

factors of 168: 1, 2, 3, 4, 6, 7, 8, 12, 14, 21, 24, 28, 42, 56, 81, 168
factors of 154: 1, 2, 7, 11, 14, 22, 77
GCD(168, 154) = 14

Why does this work? We have listed all of the *divisors* or factors of each number. We've circled all of the *common* divisors. And finally we located the *greatest* of the common factors. So we done everything required by the defintion.

2 -- Find the prime factorization of all the numbers. Select the largest power of any prime number that is a factor of all the numbers. Multiply them together. Find gcd(612, 132, 180)

$612 = 2^2 \cdot 3^2 \cdot 17$
$132 = 2^2 \cdot 3 \cdot 11$
$180 = 2^2 \cdot 3^2 \cdot 5$
so GCD (612, 132, 180) = $2^2 \cdot 3 = 12$

Why does this work? Clearly, our answer is a common divisor (a factor of both numbers) because it only has prime factors that are in common with each number. Why is it the greatest common factor? Because any factor of any common divisor must also be a factor of each number. If there were a greater common divisor, it would have a factor that is not a factor of our answer. But it must also be a factor of each of the numbers in which case it would have be included in our answer.

3 -- Later we will look at ways to compute the gcd of two numbers without factoring.

Practice Problems:

1. gcd(322, 21) gcd(90, 45, 33) gcd(625, 102)

2. You have a square pattern with which you would like to tile a room that is 203 feet by 77 feet. You want the square design to be as big as possible and you do not want any gaps or borders, the squares must exactly tessellate the area. What is the largest square pattern you can do?

LCM and Problems

Definition: The *least common multiple or* lcm of two or more non-zero numbers is the least positive integer that is a multiple all of the numbers.

There are many ways to compute the lcm of two or more numbers. You read about two different ways in *The CryptoCLub Book*. Here is another way that uses gcd:

Multiply all the number together. Then divide by the least common divisor of the numbers.

Example:

$$\text{lcm}(612,132) = \frac{612 \cdot 132}{12} = 6732$$

Why does this work? First that the answer is a multiple of both numbers: Because gcd is a divisor of each number, we can divide it out of one of the numbers in the numerator to make a whole number. The result is a multiple of the other number. In our example: we have (612/12)·132 = 51·132, a multiple of 132. or (132/12)·612=11·612, a multiple of 612. Our answer is the least of common multiples: For any smaller multiple of one of the numbers, I would have to steal a factor from the other number so the result would not be a common multiple.

1. Find the least common multiple of lcm(625, 102) using this method. Check your answer by using another method.

Problems

Do each problem in the straight-forward, tedious way. Do each problem by first computing the least common multiple of some numbers.

Long, tedious way not provided. Answers should include explanation and use of lcm.

2. At a party store, paper plates come in packages of 30, paper cups in packages of 40, and napkins in packages of 75. What is the least number of packages of plates, cups, and napkins that can be purchased so that there is an equal number of each item?
   20 packages plates, 15 packages cups and 75 packages napkins.
   The number of each item is the lcm(30,40,75)=600.
3. Two bells ring at 8:00 am for the remainder of the day, one bell rings every half hour and the other bell rings every 45 min. What time will it be when the bells ring together again?
   Answer: 9:30 How long before next ringing together is lcm(30,45)=90 minutes
4. On a string of Christmas tree lights, the red ones blink every 3 seconds, the blue ones blink every 4 seconds and the white blinks every 4.5 seconds. What is the maximum number of times they all blink together in a one-hour interval?
   100 times (or 101 if you count both the beginning and end of the hour)
   They ring together every 36 seconds = lcm(30,40,45)/10.
5. Three runners are running on a circular track. The first completes one lap every 4 minutes. The second completes one lap every 6 minutes, the third every 8 minutes. If they start together, when is the first time they get to the starting line at the same time? At that time, how may laps has each completed?
   lcm(4,6,8)=24 laps, 6, 4 and 3 laps respectively for 1st, 2nd 3rd runner.

Crickets and Chinese Remainders

Problems 1 - 5 involve several positive crickets going on a trip together. Each cricket jumps one jump in one second, so of course the cricket that jumps the longest jump will get ahead. This cricket will need to stop and wait for the other cricket to catch up from time to time to eat and sleep and talk. So the cricket needs to know which numbers to stop to wait for the slower cricket to catch up. In each case say all places where the crickets could meet up.

Challenge yourself to go past the straightforward and tedious solution for these problems.

1. A +5 cricket and a +7 cricket set off from 0.

2. A +5 cricket and a +7 cricket set off from 2.

3. A +5 cricket starts at 2 and a +7 cricket starts from 3.

4. A +4 starting at 2 and a +6 cricket starting at 1.

5. A +10 cricket starting at 9, a +9 cricket starting at 8, a +8 cricket starting at 7.

If you like these cricket problems, you might try solving the following problems by first translating into a cricket problem?

6. According to D.Wells, the following problem was posed by Sun Tsu Suan-Ching (4th century AD): There are certain things whose number is unknown. Repeatedly divided by 3, the remainder is 2; by 5 the remainder is 3; and by 7 the remainder is 2. What will be the number?

7. A woman with a basket of eggs finds that if she removes the eggs from the basket 3 at a time, there is 1 egg left. If she removes the eggs from the basket 5 at a time, there is 1 egg left. However, if she removes the eggs 7 at a time, there are no eggs left. If the basket holds no more than 100 eggs, how many eggs are in the basket?

Finding the GCD without factoring

Find the greatest common divisors of these numbers. Do not factor the numbers. Explain your reasoning.

gcd(64,62) = gcd(51, 54) = gcd(75,70) =

gcd(75,65) = gcd(55,25) = gcd(75,30) =

One general principle you might deduce from this is that subtracting one number from the other gives a number that has the same common divisors with the original numbers. We can write this as

Fact 1: For any integers a and b, $\gcd(a,b) = \gcd(b,a-b)$

Subtracting a multiple of one number from the other gives a number that has the same common divisors with the original number. This leads to the following theorem:

Fact 2: For any integers a, b and n, $\gcd(a,b) = \gcd(b,a-n\cdot b)$

We will use these facts to develop an algorithm to find the greatest common divisor of two integers. It is called the *Euclidean Algorithm*.

1. First, subtract the two numbers, then find the greatest common divisor:

gcd(106,102) = gcd(102,65) = gcd(186,175) =

2. Subtract the smaller number from the larger as many times as needed to find the greatest common divisor:

gcd(102,46) = gcd(154, 51) = gcd(165,30) =

gcd(1018,113) = gcd(572,112) = gcd(997,9) =

The Euclidean Algorithm

The Euclidean Algorithm uses repeated subtraction to find the greatest common divisor of two numbers. First we subtract the smaller number from the larger as many times as we can without "going negative." If we know the gcd of the resulting number and the smaller of the original numbers we are done. If not we repeat the step with these two smaller numbers. We may have to repeat several times but, because the numbers get smaller with each step, we will eventually get to the greatest common divisor.

We are taking advantage of the fact listed on the previous page:

For any integers a, b and n, $\gcd(a,b) = \gcd(b,a-n\cdot b)$

Example: Compute gcd(138, 120).

because 138 – 1 x 120 = 18, we know that	gcd(138, 120) = gcd(120,18) by Fact 2
because 120 – 6 x 18 = 12, we know that	gcd(120, 18) = gcd(18, 12)[1]
because 18 – 1 x 12 = 6, we know that	gcd(18, 12) = gcd(12, 6)
because 12 – 2 x 6 = 0, we know that	gcd(12, 6) = gcd(6, 0)

because gcd(6, 0) = 6, we know that gcd(138, 120) = 6

The right hand side of the algorithm is the justification. These words tell us why the algorithm eventually finds the gcd. The equations on the left form the algorithm itself. Normally this is all that you need to write down unless you wanted to explain why it works. **NOTE**: If you don't write the justification, you need to remember that the number on the right-hand side of the next to the last equation is the gcd.

Example: Compute gcd(165, 76)

165 – 2 x 76 = 13
76 – 5 x 13 = 11
13 – 1 x 11 = 2
11 – 5 x 2 = 1
2 - 2 x 1 = 0 ← can be omitted. You know to stop at 1.

conclusion: gcd(165, 76) = 1

[1] We know that gcd (18, 12) = 6, so we could stop here. But if we didn't know that we would continue as shown.

Practice with the Euclidean Algorithm

You can practice using the Euclidean Algorithm by finding the gcd of these pairs of numbers. Write the justification for the first two.

1. gcd(6, 15)

3. gcd(36, 49)

4. gcd(483, 291)

5. gcd(11413, 11289)

Now go back and find the GCD of each pair of numbers in these other two ways:

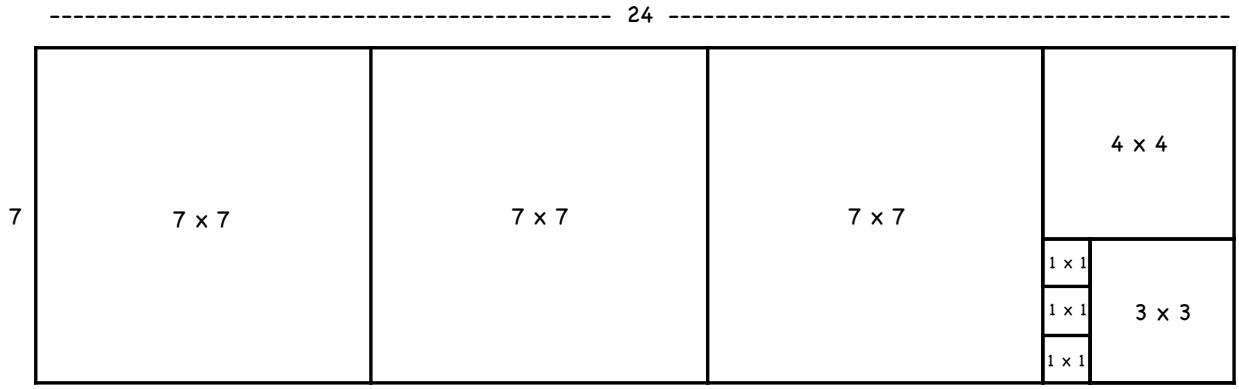
1. Write down all divisors of each number, circle the common ones, then locate the largest common one.
2. Write each one as a product of prime factors. Use the results to write the gcd as a product of primes.

In each case, which is the simplest method to use for you?

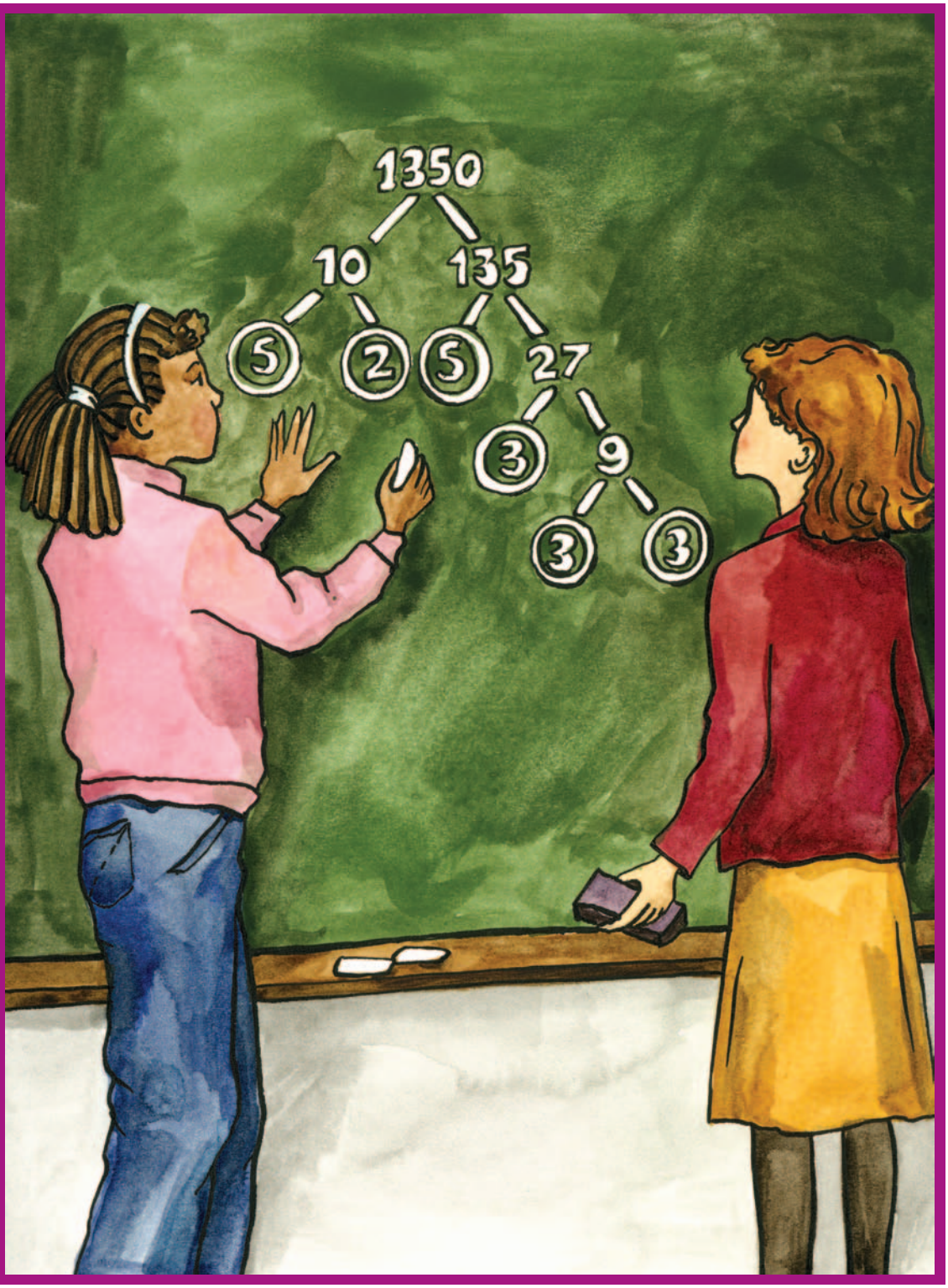
Geometry and the Euclidean Algorithm

Explain how this problem and picture shows that gcd(24,7) = 1

1. Find the largest square tile that will tile a 24 x 7 rectangle exactly



Chapter 9



Factoring

"Jesse, you learned about Vigenère ciphers in your old school, didn't you?" asked Abby. "Do you have any suggestions about how we can crack Grandfather's message?"

"We did crack some Vigenère messages, but that was quite a while ago so I don't remember all the details," admitted Jesse. "But I think we looked for patterns in the messages. Then we found common factors of some numbers related to the patterns. That helped us figure out the key length."

"It sounds like we should review what we know about factoring," said Jenny.

"That's a good idea," said Abby. "Then we'll be ready to look at the message again."

The **factors** of a number are the whole numbers that can be multiplied to get that number. For example, 3 and 4 are factors of 12 since $3 \times 4 = 12$. Other factors of 12 are 1, 2, 6, and 12.

The **multiples** of a number are the numbers you get when you multiply it by whole numbers. The multiples of 3 are 3, 6, 9, 12, and so on. A number is a multiple of each of its factors.

PROBLEMS
(Workbook page W39)

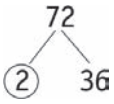
1. Find all factors of the following numbers:
   - **a.** 15
   - **b.** 24
   - **c.** 36
   - **d.** 60
   - **e.** 23
2. List four multiples of 5.
3. List all prime numbers less than 30.
4. List all composite numbers from 30 to 40.

A **prime number** is a number that has only two factors: 1 and itself. The first few prime numbers are 2, 3, 5, 7, and 11. A number that has more than two factors is a **composite number**. The first few composite numbers are 4, 6, 8, 9, and 10. The number 1 is unusual because it is neither prime nor composite.

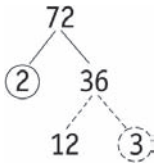
✎ **Do Problems 1–4 now.**

To factor a number means to break it into a product of its factors. There is often more than one way to do this. For example, 8×9 and 36×2 are both factorizations of 72. However, there is only one way to factor a number into prime factors, called its **prime factorization**.

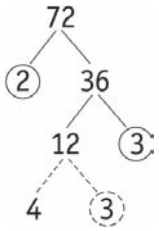
To find the prime factorization of a number, you can start with any factorization, then factor any parts of it that are not prime. One way to keep track of your work when looking for a prime factorization is to use a **factor tree**. Start with the number and break it into two factors. Circle any factors that are prime.



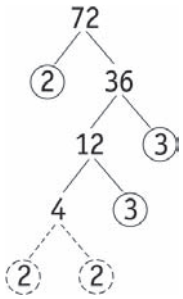
Factor each uncircled number into two factors: One way to factor 36 is 12×3. Circle the 3 to show that it is prime.



Again factor any numbers that are not prime: One way to factor 12 is 4×3. Circle the 3 since it is prime.

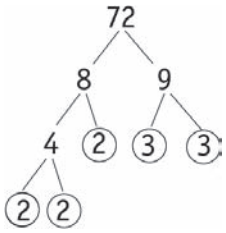


The final step is to factor 4 into 2×2 and circle the 2s.



The prime factorization of 72 is the product of all the circled numbers in the tree: $72 = 2 \times 2 \times 2 \times 3 \times 3$.

Here is another factor tree for 72. Although it is different, it gives the same prime factorization.



✎ **Do Problem 5 now.**

PROBLEMS
(Workbook page W40)

5. Use a factor tree to find the prime factorization of each of the following numbers:

a. 24 **b.** 56 **c.** 90

"A number like 72 is easy to factor," said Becky. "I already know that $72 = 8 \times 9$ since that's one of the multiplication facts. But where do I start with a larger number like 1350 that isn't in the multiplication table? How do I know any of its factors?"

It helps if you can recognize when numbers are divisible by other numbers. One way to check divisibility is to divide on a calculator. For example, 299 is divisible by 23, since $299 \div 23$ is a whole number, 13, with no remainder.

"I remember once learning about divisibility patterns," said Evie.

"You can use these patterns to tell divisibility without a calculator. If you know which numbers divide your number, you already know some of its factors. Let's make a list of rules for divisibility."

They all got to work and made a list.

"These divisibility rules will help us factor," said Evie.

RULES FOR DIVISIBILITY

- A number is divisible by 2 if it ends in 0, 2, 4, 6, or 8.
  Example: 148 is divisible by 2, but 147 is not.
- A number is divisible by 3 if the sum of its digits is divisible by 3.
  Example: 93 is divisible by 3, since 9 + 3 = 12, which is divisible by 3. However, 94 is not, since 9 + 4 = 13, which is not divisible by 3.
- A number is divisible by 4 if its last two digits form a number that is divisible by 4.
  Example: 13,5<u>48</u> is divisible by 4 since 48 is divisible by 4. But 13,5<u>10</u> is not divisible by 4 since 10 is not.
- A number is divisible by 5 if it ends in 0 or 5.
  Example: 140 and 145 are both divisible by 5, but 146 is not.

- A number is divisible by 6 if it passes the tests for divisibility by 2 and by 3.

  Example: 2358 is divisible by 6, because it is divisible by 2 (since it ends in 8) and by 3 (since 2 + 3 + 5 + 8 = 18).

- A number is divisible by 9 if the sum of its digits is divisible by 9.

  Example: The number 387 is divisible by 9 since 3 + 8 + 7 = 18, which is divisible by 9.

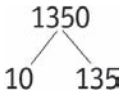
- A number is divisible by 10 if it ends in 0.

  Example: Both 90 and 12,480 are divisible by 10, but 105 is not.

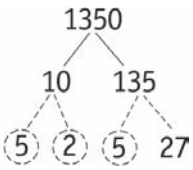
✎ **Do Problems 6–12 now.**

"OK," said Becky. "Let's try factoring a big number like 1350. Where do we start?"

"You can see right off that 1350 is divisible by 10," said Evie, "so let's start a factor tree."



"Factor the 10 as 5×2. As for the 135, I see that it is divisible by 5, so I divide 135 by 5 and get 5 and 27 as factors. After these steps, I circle all the primes: 5, 2, and 5.



PROBLEMS (Workbook pages W41–W42)

Use the rules for divisibility to answer the following questions.

6. Which of the following are divisible by 2? Why?

a. 284 **b.** 181
c. 70 **d.** 5456

7. Which of the following are divisible by 3? Why?

a. 585 **b.** 181
c. 70 **d.** 6249

8. Which of the following are divisible by 4? Why?

a. 348 **b.** 236
c. 621 **d.** 8480

9. Which of the following are divisible by 5? Why?

a. 80 **b.** 995
c. 232 **d.** 444

10. Which of the following are divisible by 6? Why?

a. 96 **b.** 367
c. 642 **d.** 842

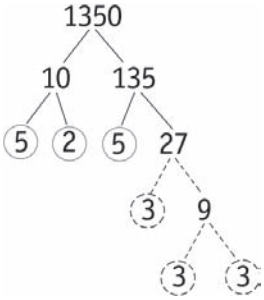
11. Which of the following are divisible by 9? Why?

a. 333 **b.** 108
c. 348 **d.** 1125

12. Which of the following are divisible by 10? Why?

a. 240 **b.** 1005
c. 60 **d.** 9900

"Next, I'll factor the 27 into 3×9 and, after that, the 9 factors into 3×3. When I am done, I circle all the primes.



"Now I multiply all the circled numbers to get the prime factorization of 1350:

$$1350 = 5 \times 2 \times 5 \times 3 \times 3 \times 3.$$

"It is easier to read if we write the primes in increasing order:

$$1350 = 2 \times 3 \times 3 \times 3 \times 5 \times 5.$$

If the same prime appears many times in a factorization, it helps to use exponents. An **exponent** tells how many times to multiply a base number. If the base is 3, then

$$3^1 = 3$$

$$3^2 = 3 \times 3$$

$$3^3 = 3 \times 3 \times 3$$

$$3^4 = 3 \times 3 \times 3 \times 3$$

$$3^5 = 3 \times 3 \times 3 \times 3 \times 3$$

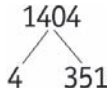
etc.

Using exponents, the prime factorization of 1350 is

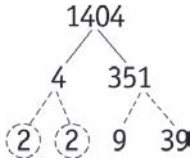
$$1350 = 2 \times 3^3 \times 5^2.$$

"Now it's your turn to find the prime factorization of a big number. How about 1404?" Evie said to Becky.

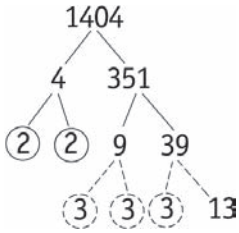
"I'll try," said Becky. "The last two digits are 04 so it is divisible by 4. I'll use that to start the tree.



"I factor the 4 into 2×2 and circle the 2s because they are prime. I see that 351 is divisible by 9 since $3 + 5 + 1 = 9$, which is divisible by 9. I divide 351 by 9 and get 39, so 351 factors into 9×39.



"I factor 9 into 3×3, and I circle each 3. I see that 39 is divisible by 3, since $3 + 9 = 12$, which is divisible by 3. So I divide 39 by 3 and get 13. Since these are prime numbers, I am done.



"I multiply all the primes together and get

$$1404 = 2^2 \times 3^3 \times 13.$$"

✎ **Do Problem 13 now.**

PROBLEMS
(Workbook pages W43–W45)

13. Use a factor tree to find the prime factorization of each of the following numbers. Write each factorization using exponents.

a. 2430 **b.** 4680
c. 357 **d.** 56,133
e. 14,625 **f.** 8550

A **common factor** of two or more numbers is a number that is a factor of each of them. For example, 3 is a common factor of 6, 9, and 15.

One way to find common factors is to list the factors of each number, then find all numbers on both lists. This works if there are not a lot of factors. For example, to find all common factors of 12 and 30, we could make two lists:

The factors of 12 are **1, 2, 3**, 4, **6**, and 12.
The factors of 30 are **1, 2, 3**, 5, **6**, 10, 15, and 30.

The numbers in bold are all the common factors. The **greatest common factor** is 6, the largest of all the common factors.

PROBLEMS
(Workbook pages W46–W47)

14. Find the common factors of the following pairs of numbers:
a. 10 and 25
b. 12 and 18
c. 45 and 60

15. Find the greatest common factor of each of the following pairs of numbers:
a. 12 and 20
b. 50 and 75
c. 30 and 45

16. For each list of numbers, factor the numbers into primes and then find all common factors for the list.
a. 14, 22, 10
b. 66, 210, 180
c. 30, 90, 210

A second way to find common factors is to find the prime factorization of each number and multiply some or all of the common prime factors. Let's use the same numbers, 12 and 30, again.

The prime factorization of 12 is **2** × 2 × **3**.
The prime factorization of 30 is **2** × **3** × 5.

The prime factorizations have 2 and 3 in common. If we multiply all the common prime factors together, we get the greatest common factor, 2 × 3 = 6. Other common factors are 1, 2, and 3.

For numbers with several factors, the second method—using the prime factorization—is usually quicker than listing all the factors of both numbers. Here is another example:

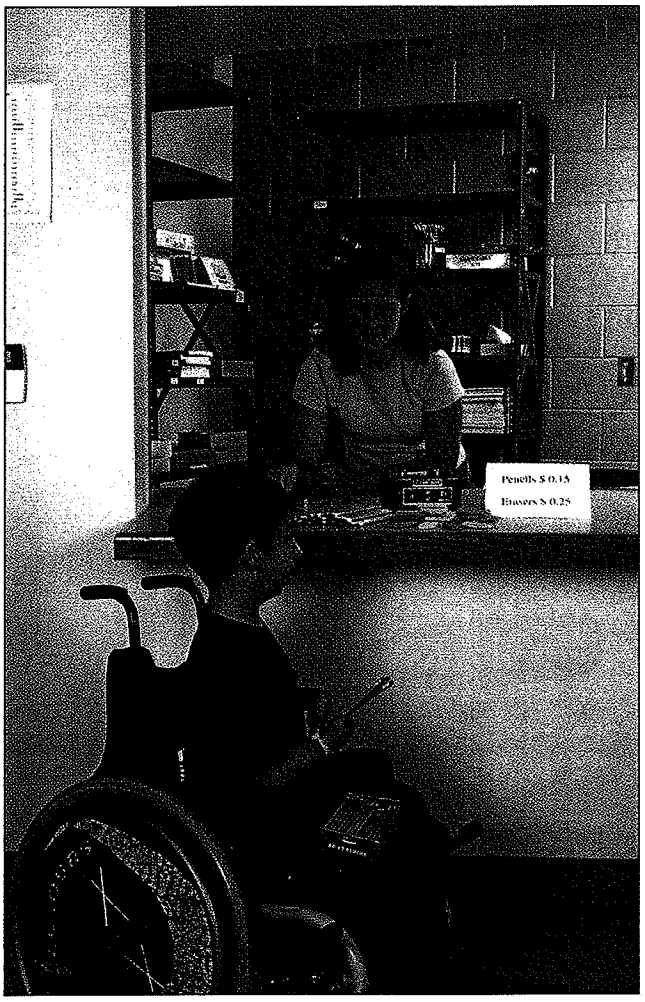
The prime factorization of 140 is **2** × **2** × **5** × 7.
The prime factorization of 60 is **2** × **2** × 3 × **5**.

The common prime factors of 140 and 60 are 2, 2, and 5. We get the greatest common factor by multiplying *all* the common prime factors, 2 × 2 × 5 = 20.

✎ **Do Problems 14–16 now.**

B Looking at Combinations

The School Store



Monica and Martin are responsible for the school store. The store is open all day for students to buy supplies. Unfortunately, Monica and Martin can't be in the store all day to take students' money, so they use an honor system. Pencils and erasers are available for students to purchase on the honor system. Students leave exact change in a small locked box to pay for their purchases. Erasers cost 25¢ each, and pencils cost 15¢ each.

1. One day Monica and Martin find $1.10 in the locked box. How many pencils and how many erasers have been purchased?

2. On another day there is $1.50 in the locked box. Monica and Martin cannot decide what has been purchased. Why?

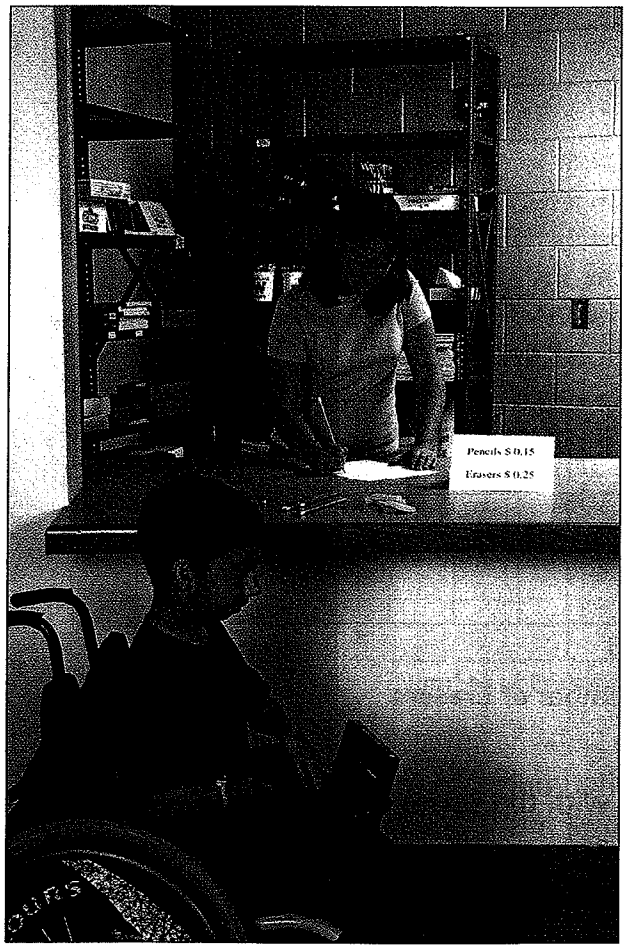
3. Find another amount of money that would make it impossible to know what has been purchased.

Monica wants to make finding the total price of pencils and erasers easier, so she makes two price lists: one for different numbers of erasers and one for different numbers of pencils.

4. Copy and complete the price lists for the erasers and the pencils.

Erasers	Price
0	$0.00
1	$0.25
2	$0.50
3	$0.75
4	$1.00
5	$1.25
6	
7	

Pencils	Price
0	$0.00
1	$0.15
2	$0.30
3	
4	
5	
6	
7	



One day the box has $1.05 in it.

5. Show how Monica can use her lists to determine how many pencils and erasers have been bought.

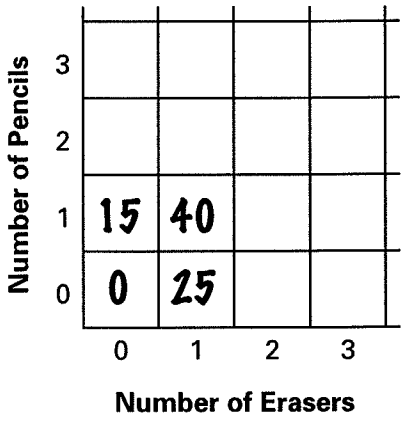
Monica and Martin aren't satisfied. Although they now have these two lists, they still have to do many calculations. They are trying to think of a way to get all the prices for all the combinations of pencils and erasers in one chart.

6. **Reflect** What suggestions can you make for combining the two lists? Discuss your ideas with your class.

B Looking at Combinations

Monica and Martin come up with the idea of a combination chart. Here you see part of their chart.

Combination Chart



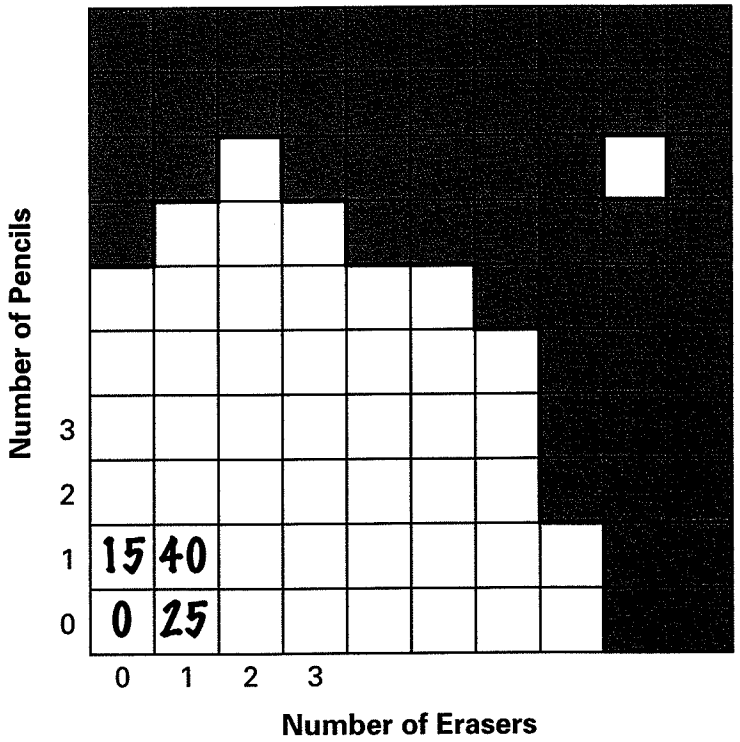
7. a. What does the 40 in the chart represent?

b. How many combinations of erasers and pencils can Monica and Martin show in this chart?

If you extend this chart, as shown below, you can show more combinations.

Use the combination chart on **Student Activity Sheet 1** to solve the following problems.

Costs of Combinations (in cents)



8. Fill in the white squares with the prices of the combinations.

9. Circle the price of two erasers and three pencils.

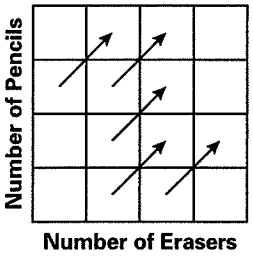
Use the number **patterns** in your completed **combination chart** on **Student Activity Sheet 1** to answer problems 10–16.

10. a. Where do you find the answer to problem 1 ($1.10) in the chart?

b. How many erasers and how many pencils can be bought for $1.10?

11. a. Reflect What happens to the numbers in the chart as you move along one of the arrows shown in the diagram?

b. Reflect Does the answer vary according to which arrow you choose? Explain your reasoning.



12. What does *moving along an arrow* mean in terms of the numbers of pencils and erasers purchased?

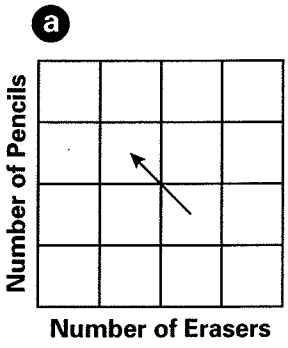
13. a. Mark on your chart a move from one square to another that represents the exchange of one pencil for one eraser.

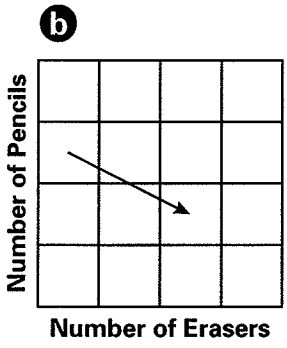
b. How much does the price change from one square to another?

14. a. Mark on your chart a move from one square to another that represents the exchange of one eraser for two pencils.

b. How much does the price change for this move?

15. Describe the move shown in charts **a** and **b** below in terms of the exchange of erasers and pencils.

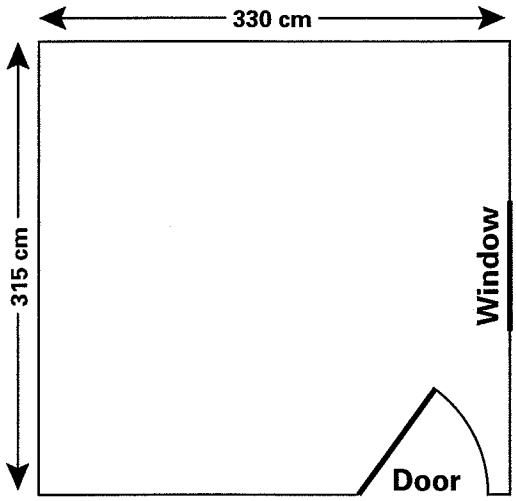




16. There are many other moves and patterns in the chart. Find at least two other patterns. Use different color pencils to mark them on your chart. Describe each pattern you find.

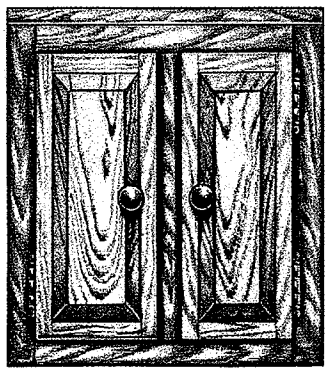
Workroom Cabinets

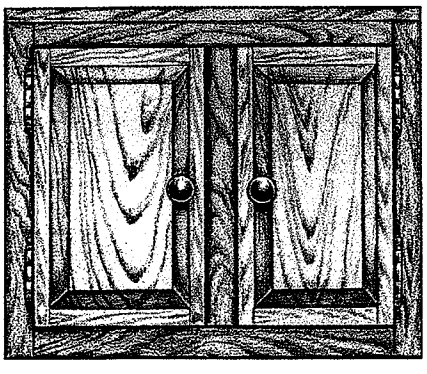
Anna and Dale are going to remodel a workroom. They want to put new cabinets along one wall of the room. They start by measuring the room and drawing this diagram.

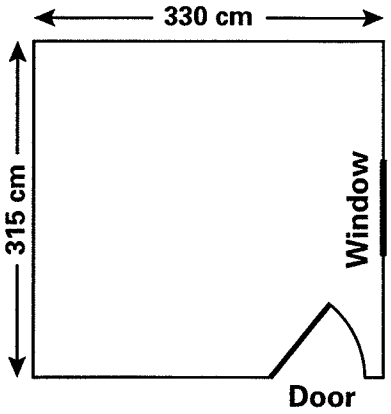


Anna and Dale find out that the cabinets come in two different widths: 45 centimeters (cm) and 60 cm.

17. How many of each cabinet do Anna and Dale need in order for the cabinets to fit exactly along the wall that measures 315 cm? Try to find more than one possibility.







Anna and Dale wonder how they can design cabinets for the longer wall.

The cabinet store has a convenient chart. The chart makes it easy to find out how many 60-cm and 45-cm cabinets are needed for different wall lengths.

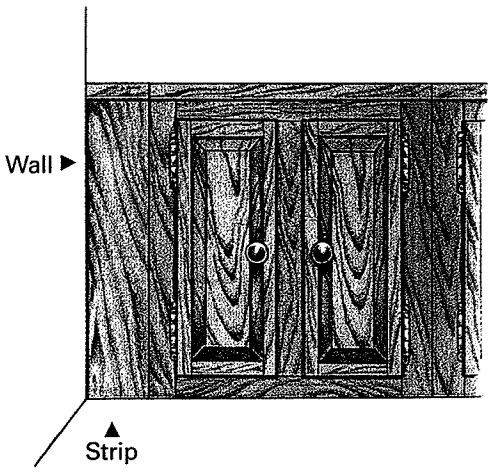
18. Explain how Anna and Dale can use the chart to find the number of cabinets they need for the longer wall in the workroom.

Lengths of Combinations (in cm)

Number of Short Cabinets	0	1	2	3	4	5	6	7	8
11	495	555							
10	450	510	570						
9	405	465	525	585					
8	360	420	480	540					
7	315	375	435	495	555				
6	270	330	390	450	510	570			
5	225	285	345	405	465	525	585		
4	180	240	300	360	420	480	540		
3	135	195	255	315	375	435	495	555	
2	90	150	210	270	330	390	450	510	570
1	45	105	165	225	285	345	405	465	525
0	0	60	120	180	240	300	360	420	480

Number of Long Cabinets

19. Can the cabinet store provide cabinets to fit a wall that is exactly 4 meters (m) long? Explain your answer.



If cabinets don't fit exactly, the cabinet store sells a strip to fill the gap. Most customers want the strip to be as small as possible.

20. What size strip is necessary for cabinets along a 4-m wall?

The chart has been completed to only 585 cm because longer rows of cabinets are not purchased often. However, one day an order comes in for cabinets to fit a wall exactly 6 m long. One possible way to fill this order is 10 cabinets of 60 cm each.

21. Reflect What are other possibilities for a cabinet arrangement that will fit a 6-m wall? Note that although you do not see 600 in the chart, you can still use the chart to find the answer. How?

Lengths of Combinations (in cm)

Number of Short Cabinets	Number of Long Cabinets: 0	1	2	3	4	5	6	7
7	315	375	435	495	555			
6	270	330	390	450	510	570		
5	225	285	345	405	465	525	585	
4	180	240	300	360	420	480	540	
3	135	195	255	315	375	435	495	555
2	90	150	210	270	330	390	450	510
1	45	105	165	225	285	345	405	465
0	0	60	120	180	240	300	360	420

On the left is a part of the cabinet combination chart.

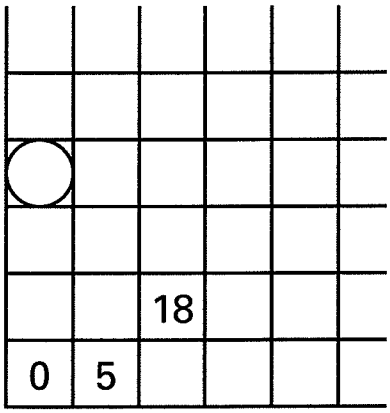
22. What is special about the move shown by the arrow?

23. If you start in another square in this chart and you make the same move, what do you notice? How can you explain this?

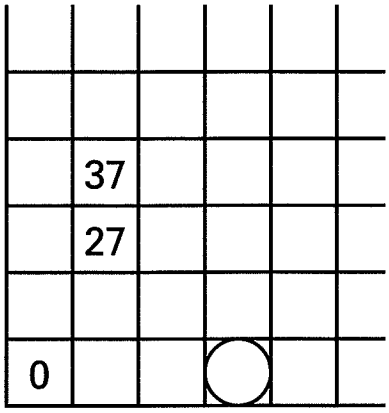
Puzzles

24. Complete the puzzles on **Student Activity Sheet 2.**

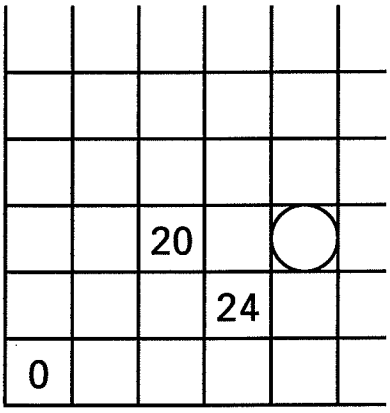
a



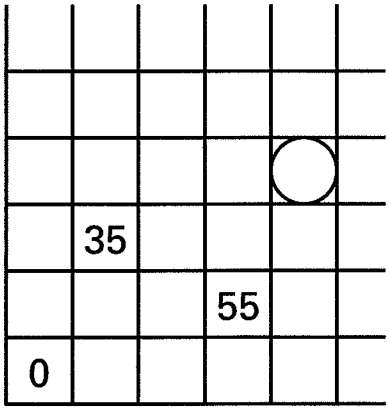
b



c



d



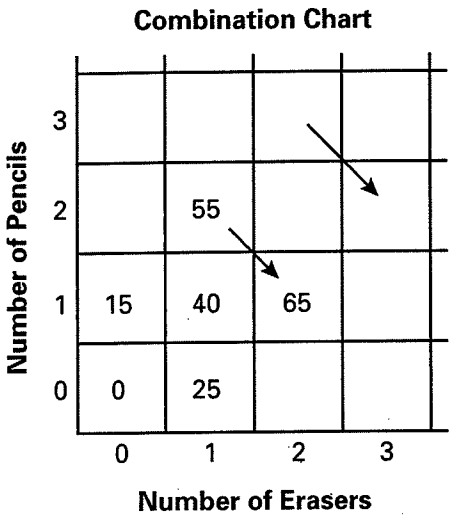
B Looking at Combinations

Summary

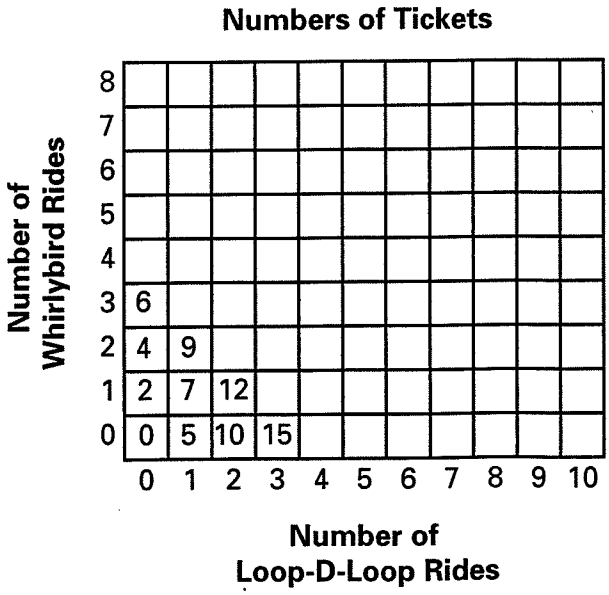
A combination chart can help you compare quantities. A combination chart gives a quick view of many combinations.

Discovering patterns within combination charts can make your work easier by allowing you to discover patterns and extend the chart in any direction.

Charts can be used to solve many problems, as you studied in "The School Store" and "Workroom Cabinets." In this chart the arrow represents the exchange of one pencil for one eraser.



Check Your Work



This year the school fair has two rides. The Loop-D-Loop costs five tickets, and the Whirlybird costs two tickets.

1. In your notebook, copy the combination chart that shows how many tickets are needed for different combinations of these two rides. Complete the chart as necessary to solve the word problems.

2. How many tickets are needed for two rides on the Loop-D-Loop and three rides on the Whirlybird?

3. Janus has 19 tickets. How can she use these tickets for both rides so that she has no leftover tickets?

4. **a.** On your combination chart, mark a move from one square to another that represents the exchange of one ride on the Whirlybird for two rides on the Loop-D-Loop.

   b. How much does the number of tickets as described in 4a, change as you move from one square to another?

5. Use the combination chart on **Student Activity Sheet 3.**

   a. Write a story problem that uses the combination chart.

   b. Label the bottom and left side of your chart. Give the chart a title and include the units.

   c. What do the circled numbers represent in your story problem?

50	52	54	56	58	60
40	42	44	46	48	50
30	32	34	36	38	40
20	22	24	26	28	30
10	12	14	16	18	20
0	2	4	6	8	10

For Further Reflection

Do you think combination charts will always have a horizontal and vertical pattern? Why or why not? What about a pattern on the diagonal?

Combination Charts

A *n,m Combination Chart* is created on a grid by entering 0 into an initial box and adding *n* for each step to the right (in the positive *x*-direction) and adding *m* for each step up (in the positive *y*-direction). Combination Charts can also be extended backwards to include negative combinations downwards and to the left. It is called a combination chart because each entry is a combination of the two numbers *n* and *m*. That is, the number in any square is

n x (the number of steps to the right from 0) + *m* x (the number of steps up from 0)

Notice: Each row going right and each column going up in a combination chart is an arithmetic sequence. When the chart is continued to include negative combinations, each row and each column is an arithmetic progression. Notice also that any diagonal also form an arithmetic progression.

10	13	16	19	22	25	28	31	34	37	40
5	8	11	14	17	20	23	26	29	32	35
0	3	6	9	12	15	18	21	24	27	30
-5	-2	1	4	7	10	13	16	19	22	25
-10	-7	-4	-1	2	5	8	11	14	17	20
-15	-12	-9	-6	-3	0	3	6	9	12	15
-20	-17	-14	-11	-8	-5	-2	1	4	7	10
-25	-22	-19	-16	-13	-10	-7	-4	-1	2	5
-30	-27	-24	-21	-18	-15	-12	-9	-6	-3	0
-35	-32	-29	-26	-23	-20	-17	-14	-11	-8	-5
-40	-37	-34	-31	-28	-25	-22	-19	-16	-13	-10

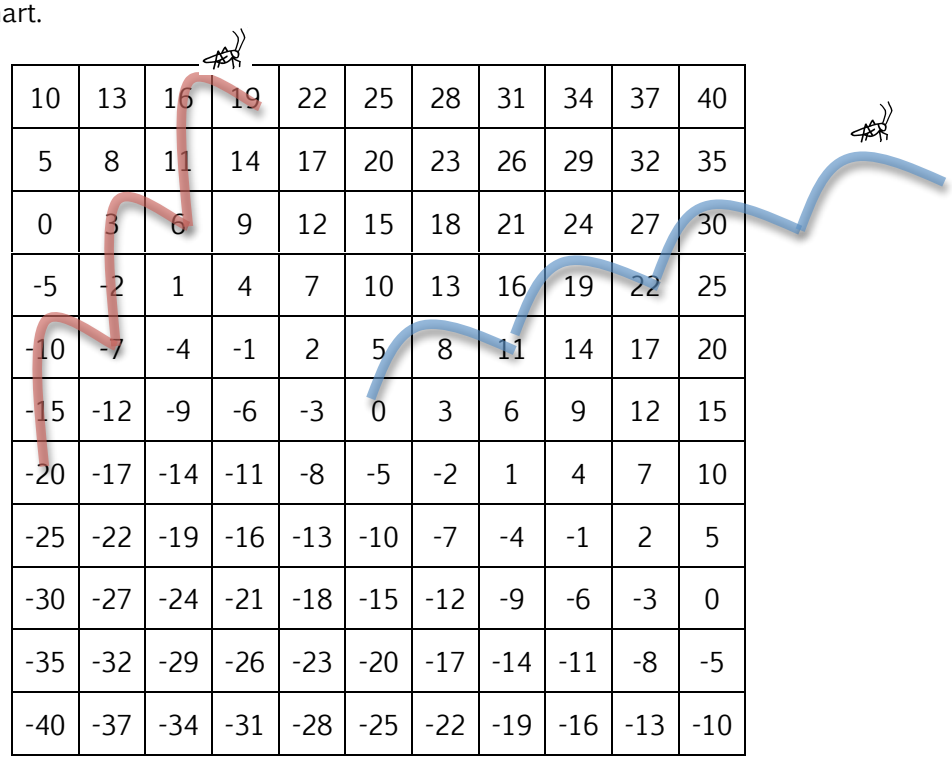
This shows part of a 3,5 *combin*ation Chart. The shaded part contains positive combinations of *n* and *m*. Going down from the shaded region, combinations have negative multiples of 5. Going left of the shaded region, combinations have negative multiples of 3.

Example combinations: $25 = 5 \times 3 + 2 \times 5$ $\quad -12 = 1 \times 3 + (-3) \times 5$

$1 = (-3) \times 3 + 2 \times 5$ $\quad -22 = (-4) \times 3 + (-2) \times 5$

Arrows: We use arrows to talk about moving about on a combination chart. → means move one unit to the right. ↑ means move one unit up. ← means move one unit to the left. ↓ means move one unit down.

Crickets: A cricket jumping around on a combination chart is named by how many boxes it goes to the right and how many boxes it goes up on each jump. A →→↑ cricket moves two to the right and one up on every jump. On a 3,5 combination chart would jump from 0 to 11 to 22, as shown on this chart.



10	13	16	19	22	25	28	31	34	37	40
5	8	11	14	17	20	23	26	29	32	35
0	3	6	9	12	15	18	21	24	27	30
-5	-2	1	4	7	10	13	16	19	22	25
-10	-7	-4	-1	2	5	8	11	14	17	20
-15	-12	-9	-6	-3	0	3	6	9	12	15
-20	-17	-14	-11	-8	-5	-2	1	4	7	10
-25	-22	-19	-16	-13	-10	-7	-4	-1	2	5
-30	-27	-24	-21	-18	-15	-12	-9	-6	-3	0
-35	-32	-29	-26	-23	-20	-17	-14	-11	-8	-5
-40	-37	-34	-31	-28	-25	-22	-19	-16	-13	-10

Notice: Any cricket jumps out an arithmetic sequence.

Example: A →↑↑ cricket starting on a -21 on the 3,5 Combination Chart will jump out the sequence

-20, -7, 6, 19, 32, . . .

adding +13 = 3 + 2 x 5 (3 for the → and 5 for each ↑) with each jump. If the same cricket starts on a -6 it hops out the sequence

-6, 2, 15, 28, 41, . . .

still adding +13 with each jump. Notice a formula for this cricket's jumps is -6 + 8*n*, where *n* is the number of jumps since 6.

1. Describe with arrows the cricket on the 3,5 combination chart that jumps out the sequence 0, 2, 4, 6, 8, . . . : all even numbers.

2. Describe with arrows the cricket on the 3,5 combination chart that jumps out the sequence 9, 23, 37, . . . : 9 + *17n*, where *n* is number of jumps since 9.

3. Write a formula for a ↑←← cricket that starts on 12. Be sure to say what your variable means.

Combination Chart Problems

1. Which of the following numbers appears on a 3,5 combination chart. If possible, describe a cricket that jumps from 0 to each number in one jump.

95

126

-97

2. Which of the following numbers appears on a 4,6 combination chart. If possible, describe a cricket that jumps from 0 to each number in one jump.

95

126

3. On a 6, 8 Combination Chart will a →→↑cricket, starting on a 12, ever land on 1027?

No, explanations vary: this cricket jumps +20 each jump and 1027 is not 12 more than a multiple of 1027

On the same chart, describe a cricket that starts at 12 and next lands on another 12.

←←←←↑↑↑ = $\leftarrow^{4}\uparrow^{3}$ *is one way. NOTE: 12 + 6·(-4)+8·4 = 12*

4. On a 1, 5 combination chart describe arrows for a +22 cricket, a +38 cricket, a -24 cricket? Describe a procedure for finding the arrows for any size cricket.

+22 →→↑↑↑↑ = 2·1+4·5

+38 →→→↑↑↑↑↑↑↑ = 3·1 + 6·5

-24 ←←←←← ↓↓↓↓=-4·1+ (-4)·5 or ↓↓↓↓↓→ = 1 + (-5) ·5

For any number, divide by 5. The quotient is the number of ↑ and the remainder is the number of →

5. On a 4, 7 combination chart describe the arrows that make a +1 cricket. Is it possible to make a +1 cricket on a 4, 6 combination chart?

→→↓ = 2·4+(-1)·7 = +1

not possible on 4,6 chart because all the numbers on the chart are even numbers.

6. On an *n, m* combination chart find arrows that make a +0 cricket.

m x n – n x m = 0.

7. Complete the rest of this section of a combination chart.

	181			
			172	
109				

ONE WAY: (172-109)/3 = 21, so diagonal is +21 cricket. Then it is easy to get an up arrow

Show how to solve this problem by solving equations.

Let x amount of → and y be amount of ↓ then solve these tow equations:

109 + 3x + 3y = 172

109 + x + 4y = 181

Make an EXCEL version of this combination chart that includes a space that contains zero.

You will be very happy if you figure out how to use EXCEL to make combination charts.

8. Make your own combination chart problem:

Solving $A{\cdot}x + B{\cdot}y = gcd(A,B)$

In the equation, $A{\cdot}x + B{\cdot}y = \gcd(A,B)$, A and B are fixed numbers and we want to find a combination of the two that is equal to their greatest common divisor.

Example: Find x and y such that $11x + 3y = 1$. [Note gcd(11,3) = 1] We proceed through the Euclidean Algorithm but we keep careful track of the combinations of 11 and 3. Using arrows helps:

$11 - 3{\cdot}3 = 2$	$2 = \uparrow\leftarrow\leftarrow\leftarrow$	$= \uparrow\leftarrow^{3}$	or $11{\cdot}(1) + 3{\cdot}{-3} = 2$
$3 - 1{\cdot}2 = 1$	$1 = \rightarrow \downarrow\rightarrow\rightarrow\rightarrow$	$= \downarrow\rightarrow^{4}$	or $11{\cdot}(-1) + 3{\cdot}4 = 1$ ←
$2 - 2{\cdot}1 = 0$	$0 = \uparrow\leftarrow^{2} -2(\downarrow\rightarrow^{4})$	$= \uparrow^{3}\leftarrow^{11}$	or $11{\cdot}(3) + 3{\cdot}{-11} = 0$

solution: $x = -1$, $y = 4$

Just by looking at our work, we can find solutions to more equations with the same coefficients. For example, $x = 1$, $y = -3$ is a solution of the equation $11x + 3y = 2$. As can be seen in the first row of the algorithm.

We can also find a solution to $11x + 3y = c$, for any integer c, just by multiplying the solution above by c. That is, $x = -c$, y = 4c is a solution. This can be seen by plugging the values back into the equation and using the distributive rule to simplify:

$$11(-c) + 3(4c) = c{\cdot}(11(-1) + 3(4)) = c{\cdot}1 = c$$

Another example: Find x and y such that $27x + 15y = 3$. Notice that 3 is the gcd(27,3) so when we do the Euclidean algorithm we will eventually get a 27,15 combination that equals 3. We proceed then with the Euclidean Algorithm, again keeping careful arrow-track of the remainders:

$27 - 1{\cdot}15 = 12$	$12 = \uparrow\leftarrow$	$= \uparrow\leftarrow$	or $27{\cdot}(1) + 15{\cdot}{-1} = 12$
$15 - 1{\cdot}12 = 3$	$3 = \rightarrow \downarrow\rightarrow$	$= \downarrow\rightarrow^{2}$	or $27{\cdot}(-1) + 15{\cdot}{-2} = 3$ ←
$12 - 4{\cdot}3 = 0$	$0 = \uparrow\leftarrow \uparrow^{4}\leftarrow^{8}$	$= \uparrow^{5}\leftarrow^{9}$	or $27{\cdot}(5) + 15{\cdot}{-9} = 0$

solution: $x = -1$, $y = 2$

What is a solution to the equation $27x + 15y = -3$? $x =$ _____ , $y =$ _____

What is a solution to the equation $27x + 15y = 12$? $x =$ _____ , $y =$ _____

What is a solution to the equation $27x + 15y = 9$? $x =$ _____ , $y =$ _____

What is a solution to the equation $27x + 15y = 11$? $x =$ _____ , $y =$ _____

What is a solution to the equation $27x + 15y = 0$? $x =$ _____ , $y =$ _____

It is always possible to solve the equation, $A{\cdot}x + B{\cdot}y = \gcd(A,B)$ with this method because the gcd(*A*,*B*) will always appear when we do the Euclidean Algorithm. This procedure for finding the

solutions to this type of equation is called the Extended Euclidean Algorithm.

Observation 1 The gcd(*A,B*) will always appear on a *A,B* **combin**ation chart. We have shown that using the Extended Euclidean Algorithm you can always find a combination, $A \cdot x + B \cdot y$, that is equal to gcd(*A,B*).

Problem: Locate 1 [= gcd(4,7)] on a 4,7 combination chart. Only part of the chart is shown:

35	39	43	47	51	55
28	32	36	40	44	48
21	25	29	33	37	41
14	18	22	26	30	34
7	11	15	19	23	27
0	4	8	12	16	20

Observation 2 Only multiples gcd(*A,B*) will appear on a *A,B* **combin**ation chart. Only multiples of 3 [= gcd(6,9)] appear on this 6,9 combination chart even if it were continued forever in all directions.

24	30	36	42	48	54
15	21	27	33	39	45
6	12	18	24	30	36
-3	3	9	15	21	27
-12	-6	0	6	12	18
-21	-15	-9	-3	3	9

Example: There are only even numbers on a 4,6 combination chart because 4 and 6 are even so any combination must also be even. On a 4,8 combination chart, not only are all the numbers even but they are also all multiples of 4. This is because both 4 and 8 are multiples of 4. So, of course, any combination of 4 and 8 must also be a multiple of 4.

Observation 3 All of the multiples of gcd(*A,B*) will appear on a *A,B* **combin**ation chart. If a number is equal to $c \cdot$ gcd(*A,B*), just take a combination that equals gcd(*A,B*) multiply by *c*. In particular, if gcd(*A,B*) = 1, all numbers will appear somewhere on the chart.

Problem: Where is 37 on the 4,7 combination chart, part of which is shown at the top of the page?

Extended Euclidean Algorithm Worksheet

Doing the extended algorithm on this worksheet, instead of working with arrows will help to understand the TI-84 program that we will write for finding the gcd and solving equations like

A – (B * Q) = R			X	Y
			R = A*X +	B*Y
		A	1	0
		B	0	1
		Q=int(A/B)	R=A-Q*B	X2-Q*X1	Y2-Q*Y1
A=	B=				

TI-84 Program for finding gcd(*A*,*B*) and solutions to $Ax + By = \gcd(A,B)$

To enter this program into your TI-84 Calculator follow these steps:
Press PRGM NEW
Press ENTER
Type in a program name when prompted by NAME= . Suggestion: EEA
Press ENTER
Enter these commands:

Input "A=", A Input "B=", B	These commands will display A= and then B= as prompts to enter A and B
0→V 1→X 0→Y 1→H	The program repeated updates R, X, Y so that R=A*N+B*M starting with B = A*0+B*1 V and H are X and Y one step back to R.
B→R	B is the first R
While R>0	The "while . . . end" is a loop. This part of the code will repeat the Euclidean algorithm step until R = 0.
B→G	First, we store B into G. This is a housekeeping trick that will make more sense once the whole loop is understood. G will eventually hold the gcd(A, B).
int(A/B)→Q A-Q*B→R	The next two steps compute Q and R in the next step of the Euclidean Algorithm: A - Q x B = R.
V→T N-Q*V→V T→X H→T M-Q*H→H T→Y	Next we compute the number of A's and B's in the combination for the new R. Notice how we save V in a temporary location, T, and make a new value for H. Repeat the steps for the right-left arrows.
B→A R→B	We get ready for the next step by moving B to A and R to B.
End	This marks the end of the "while" loop
Disp G Disp X,Y	We display our answers. First, the greatest common divisor of A and B, gcd(A,B) Then the calculated solution to AX+BY=gcd(AB)
Stop	

.

More Diophantine Equations to Solve

Some of these equations do not have the same form as $Ax + By = \gcd(A,B)$. You must modify your thinking to find solutions. Determine whether the equation has a solution. If it does, write down two different solutions. Remember, we are only looking for integer solutions. You may want to use the calculator program for at least some of the problems.

Things that happen: 1 -- RHS is not gcd. IT may be a multiple of the gcd, in which case there are solutions. If it is not a multiple of the gcd, there will be no solution. 2 – The larger of the two coefficients does not appear first. 3 – There is subtraction instead of addition. 4 – variable names change.

1. $456x+295y = 1$
2. $221x+24y = 3$
3. $292x-468y = 2$
4. $3728y+2831x = 1$
5. $68x+172y = 8$
6. $401x-34y = 1$
7. $3625x+2534y = 1$
8. $1113x+1102y=1$
9. $456x-295y = 2$
10. $24x+221y = 0$
11. $342x-148y = 15$
12. $311x-129y=2$

Combination Chart Problems

1. In a football game, a touch down with an extra point is worth 7 points and a field goal is worth 3 points. Suppose that in a game the only scoring done by teams are touchdowns with extra points and field goals. Which of the scores from 1 to 25 are impossible for a team to score? List all ways for a team to score 40 points.

2. Joe counts 48 heads and 134 legs among the chickens and dogs on his farm. How many dogs and how many chickens does he have?

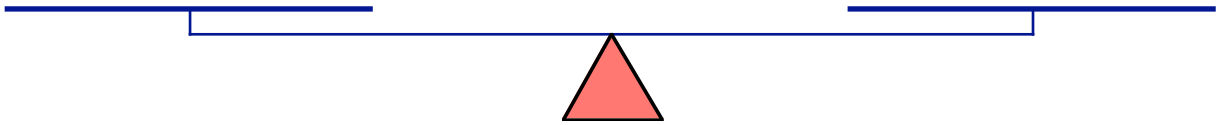
3. A customer wants to mail a package. The postal clerk determines the cost of the package to be $2.86, but only 6¢ and 15¢ stamps are available. Can the available stamps be used for the exact amount of the postage? Why or why not?

4. I only have 5¢ and 13¢ stamps. Which of the following postages costs can be made exactly using these stamps: 6¢, 25¢, 37¢, $1.16. What is the largest postage that cannot be made exactly with these stamps?

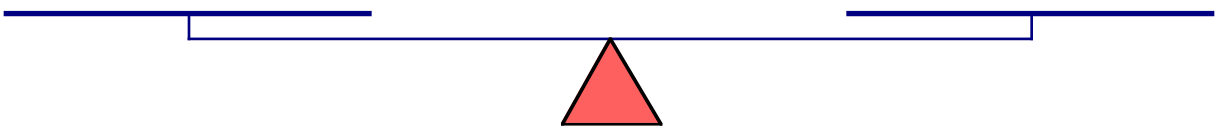
5. **Challenge**: I only have 31¢ and 37¢ stamps. What is the largest postage that cannot be made using only these stamps?

Combination Chart Problems with Negative Numbers

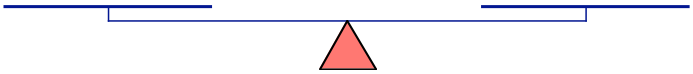
6. Terry has some 5 oz. weights, some 7 oz weights and a two-pan balance. Show how she can weigh out 1 ounce, 2 ounces, 3 ounces, 4 ounces, 11 ounces and 12 ounces chocolates. For example, she could put a 5 oz. weight on one side of the balance and a 7 oz weight on the other side; then she could add chocolate to the 5-oz side until it balanced the other side. Is there any weight she could not weigh out given that she has sufficient 5-oz and 7-oz weights?

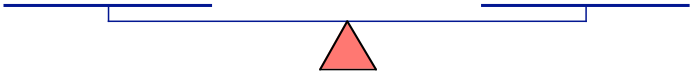


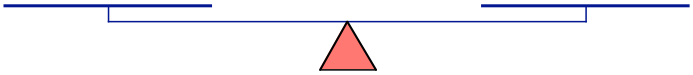
7. You have some 12 oz. weights, some 15 oz weights and a two-pan balance. Describe all of the other weights can you determine?



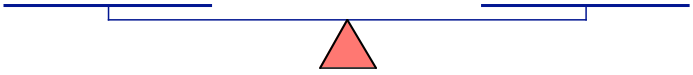
°

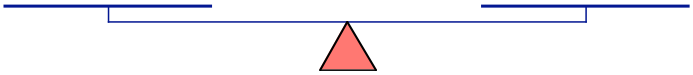


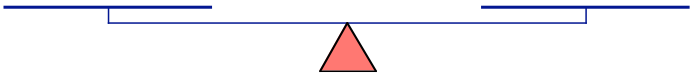




°







Teaching Presentation: Modular Arithmetic

1. Read Chapter 11, Modular Arithmetic and 12, Applications of Modular Arithmetic from *Crypto Club: Making Breaking Secret Codes*. Do all of the activities and problem.

2. You will be assigned one of the sets of problems these Chapters to present to the class.:

Chapter 11:
- 1- 6 Clock arithmetic
- 7 – 11 24-hour clock
- 12 – 13 intro to modular arithmetic
- 15 – 16 equivalent numbers
- 18 – 24 reducing
- CLASS ACTIVITY: page 111

Chapter 12:
- 1- 3 relation to multiplicative cipher
- 4 – 5 reducing mod 26
- 12 – 13 intro to modular arithmetic
- 6 – 8 reducing mod 26
- 9 Tim's shortcut for reducing
- 10 – 15 Calculator applications

The problems are available separately in a workbook, provided on the webpage. You need not do them on these pages but you can if you wish.

3. Make up more advanced problems that you think will help the class better understand what we are doing in class.

Complete the back of this sheet and write the solutions to all the problems in your assigned section. Hand in one copy and keep a copy for yourself. The class period after the proposal is due you will be expected to present the problem to a class instructor. The instructor will pass you as ready or not to present to the class. Very unfortunately, there will not be time for everyone to present. For some people their presentation grade from the practice presentation will also be their class presentation grade.

assignment	date	grade
Proposal		/20
Group Practice Presentation		/10
Class presentation		/10
Related Problems		/10

Pink Sheet: Modular Arithmetic

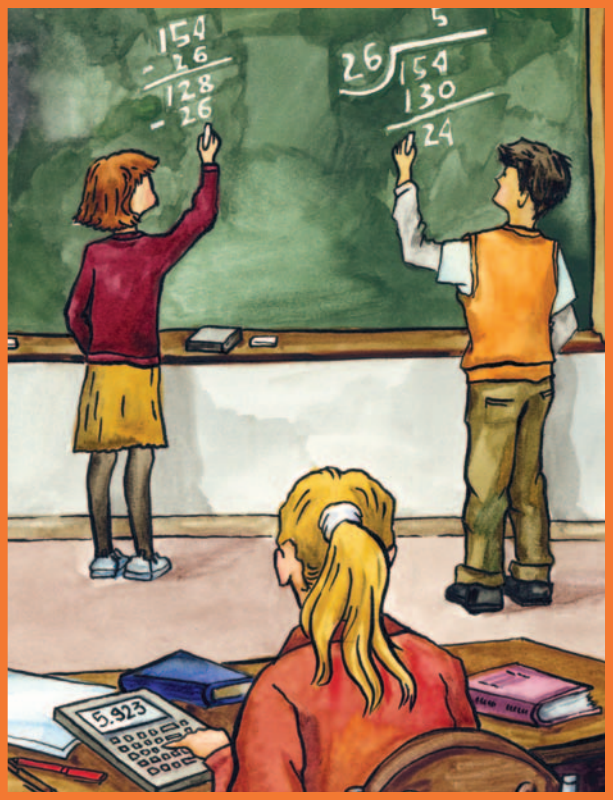
Name: Date:

1. State the problems you were assigned from *Cryptoclub*::

2. State your related, advanced problems

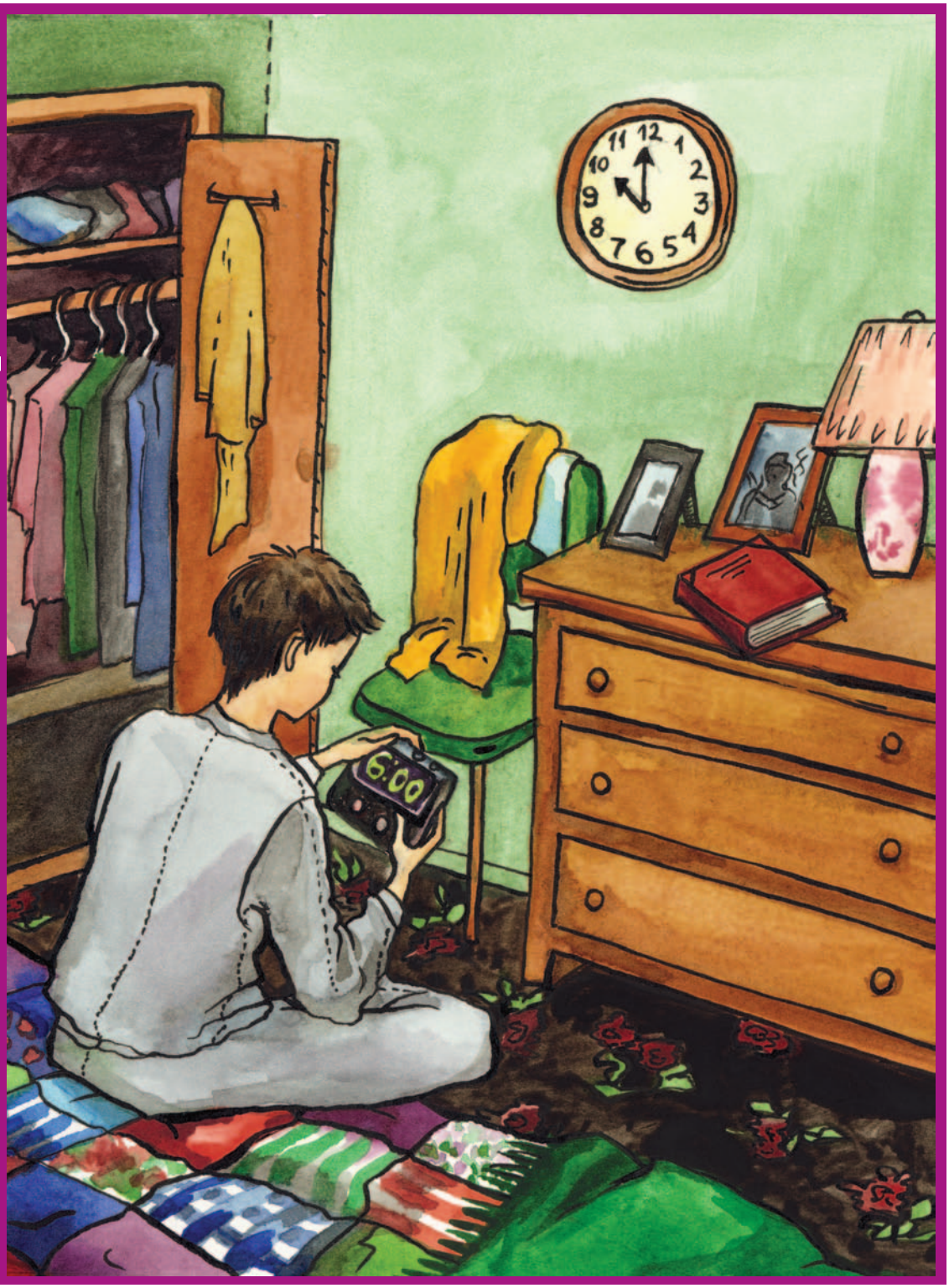
3. Provide solutions to all the problems on separate sheets of paper

Unit 4



Modular (Clock) Arithmetic

Chapter 11

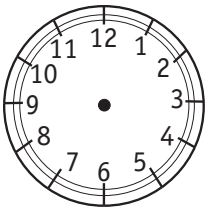


Introduction to Modular Arithmetic

Tim was always asking questions. He wondered about the reasons things are the way they are. He often asked, "Why?" Usually his teacher encouraged his curiosity, but one busy day she just didn't have time. When Tim asked another one of his questions, she answered him in a frustrated way. "Tim," she said, "some things are *always* true. You just have to accept that." Then she continued, "2 plus 2 is *always* 4, 4 plus 4 is *always* 8, and 8 plus 8 is *always* 16."

Instead of accepting what his teacher said, Tim took her words as a challenge. He was determined to think of an example to prove that the things she had listed are *not* always true. He started thinking about arithmetic, hoping to come up with an example. He was still thinking about it as he got ready for bed that night. "It's 10 PM now," he said. "If I want to sleep for 8 hours, I should set my alarm to wake me up at 6 AM."

"That's it! In clock arithmetic, 10 PM + 8 hours = 6 AM. So 10 + 8 is *not* always 18! My teacher said 8 plus 8 is *always* 16, but in clock arithmetic 8 + 8 = 4. I can't wait to tell her tomorrow!"



Tim reported his example to his class the next day. They all agreed that addition in clock arithmetic is pretty strange. When the sum is less than 12, clock addition is just like regular addition. For example, 6 + 3 = 9. But when the sum is greater than 12, we start counting again with 13 equal to 1. For example, 6 + 7 = 1 (in clock arithmetic).

✎ **Do Problems 1–6 now.**

PROBLEMS
(Workbook page W67)

1. Lilah had a play rehearsal that started at 11:00 AM on Saturday morning. The rehearsal lasted three hours. What time did it end?
2. Peter was traveling with his family to visit their grandmother and their cousins, Marla and Bethany, near Pittsburgh. The car trip would take 13 hours. If they left at 8:00 AM, at what time would they arrive in Pittsburgh?
3. The trip to visit their other grandmother takes much longer. First they drive for 12 hours, then stop at a hotel and sleep for about 8 hours. Then they drive about 13 hours more. If they leave at 10:00 AM on Saturday, when will they get to their grandmother's house?
4. Use clock arithmetic to solve the following:

   a. 5 + 10 = ___ **b.** 8 + 11 = ___

   c. 7 + 3 = ___ **d.** 9 + 8 + 8 = ___
5. Jenny's family is planning a 5-hour car trip. They want to arrive at 2 PM. At what time should they leave?
6. In Problem **5**, we moved backward around the clock. This is the same as subtracting in clock arithmetic. Solve the following subtraction problems using clock arithmetic. Use the clock, if you like, to help you:

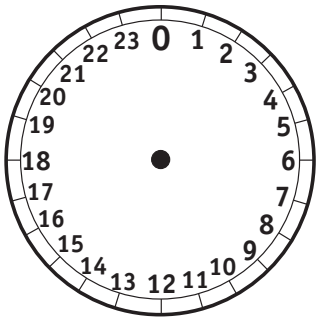
   a. 3 – 7 = ___ **b.** 5 – 6 = ___

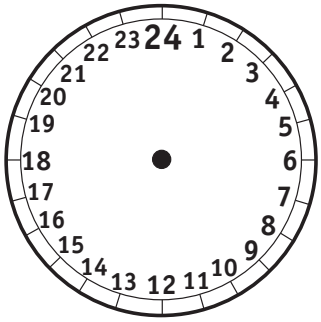
   c. 2 – 3 = ___ **d.** 5 – 10 = ___

24-Hour Time

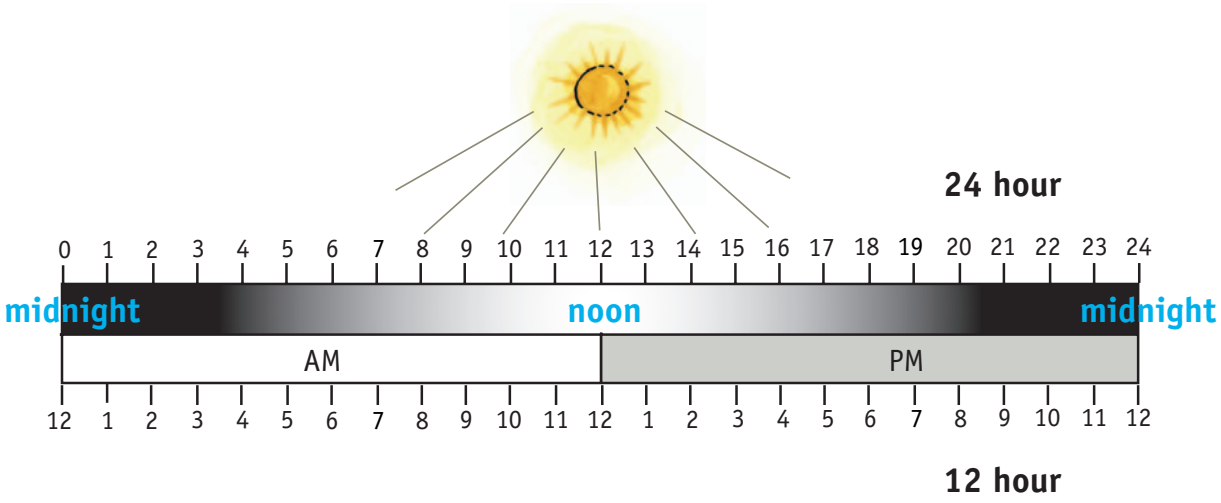
Peter asked Abby one of his favorite old riddles. "What time is it when the clock strikes thirteen?" Abby thought about it, but had no idea of the answer—all of the clocks in her house only went up to twelve. "It is time to get a new clock," he said.

Peter's riddle assumes that a clock that has a 13 on it must be broken. But actually, there are clocks that have numbers for all of the 24 hours in the day.





On a **24-hour clock**, a different number is used for every hour. The hours before noon are numbered from 1 to 12 as usual, but the afternoon and evening hours are different—they are numbered from 13 to 24. So, 13:00 hours means 1 PM, 14:00 hours means 2 PM, and so on, up to 24:00 hours. Midnight can be numbered either 0 or 24.



With a 24-hour clock, you don't need to say AM or PM—you can tell whether the time is AM or PM simply by whether it is less than or greater than 12.

It is not hard to convert between 12-hour and 24-hour time. Morning hours are the same in both systems. To convert afternoon and evening hours, you just have to add or subtract 12.

For example, to convert 9 PM to 24-hour time, add: 9 + 12 = 21. So, 9 PM is the same as 21:00 hours.

To find 16:00 hours in 12-hour time, subtract: 16 – 12 = 4. So, 16:00 hours is the same as 4 PM.

The 24-hour system is widely used in Europe and is becoming increasingly common in the United States. It is often used for train and bus schedules to avoid confusion. Sometimes it is called "military time" because it is the system used by military agencies.

✎ **Do Problems 7–11 now.**

PROBLEMS
(Workbook pages W68–W69)

7. Write the following 12-hour times using the 24-hour system:

a. 3 PM **b.** 9 AM **c.** 11:15 PM

d. 4:30 AM **e.** 6:45 PM **f.** 8:30 PM

8. Write the following 24-hour times as 12-hour times, using am or pm.

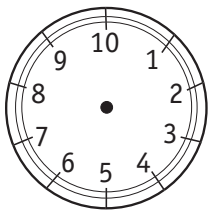
a. 13:00 **b.** 5:00 **c.** 19:15

d. 21:00 **e.** 11:45 **f.** 15:30

9. Use clock arithmetic on a 24-hour clock to solve the following:

a. 20 + 6 = _____ **b.** 11 + 17 = _____

c. 22 – 8 = _____ **d.** 8 – 12 = _____



10. Solve the following on a 10-hour clock:

a. 8 + 4 = _____ **b.** 5 + 8 = _____ **c.** 7 + 7 = _____

d. 10 + 15 = _____ **e.** 6 – 8 = _____ **f.** 3 + 5 = _____

11. Challenge: Is 2 + 2 always 4? Find a clock for which this is not true.

Modular Arithmetic

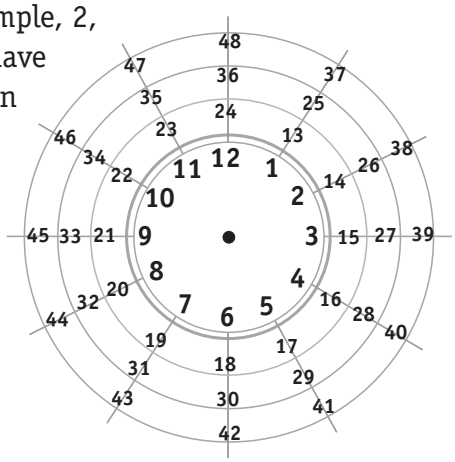
Tim wrote down the answers to some of his clock arithmetic problems. Abby saw his calculations.

"What has happened to you?" she said. "These answers are all wrong!"

"The answers aren't wrong," said Tim defensively. "I'm not using regular arithmetic. There must be some way to write these problems to make it clear that I did them in clock arithmetic."

Their teacher showed them a way. She told them that another term for clock arithmetic is **modular arithmetic**. The word "modulus," or the shorter word "mod," is used to show which size clock to use. For example, the expression "mod 12" means use a 12-hour clock, "mod 10" means use a 10-hour clock, and so on. We could write the answer to the problem $8 + 4 =$ ____ as $8 + 4 = 2 \pmod{10}$ to make it clear that we used clock arithmetic.

To understand modular arithmetic, it helps to understand which numbers have the same position on your clock. For example, 2, 14, 26, and 38 all have the same position on the 12-hour clock.



✎ **Do Problems 12–14 now.**

PROBLEMS (Workbook page W70)

12. **a.** The figure shows numbers wrapped around a 12-hour clock. List all numbers between 1 and 48 that have the same position on a 12-hour clock as 3.

b. If the number wrapping continues, what numbers between 49 and 72 would have the same position on a 12-hour clock as 3?

13. **a.** List all numbers between 1 and 48 that have the same position on a 12-hour clock as 8.

b. If the number wrapping continues, what numbers between 49 and 72 would have the same position on a 12-hour clock as 8?

14. **a.** How can you use arithmetic to describe numbers that have the same position on a 12-hour clock as 5?

b. What numbers between 49 and 72 have the same position on the 12-hour clock as 5?

There is a special term in modular arithmetic to describe numbers that have the same position on a clock. Two numbers are **equivalent mod n** if they differ by a multiple of n—in other words, if they have the same position on a clock of size n. For example, 37 and 13 are equivalent mod 12 because their difference, 37 – 13 = 24, is a multiple of 12.

The symbol "≡" means "is equivalent to." Using this notation,

$$37 \equiv 13 \pmod{12}.$$

This notation includes mod 12 in parentheses to tell us what clock the numbers are on.

The symbol "≡" reminds us of the equal sign "=" but it is a little different. Equivalent numbers are alike because they have the same position on the clock, but they don't have to be equal, so we use a slightly different symbol.

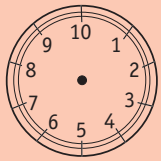
PROBLEMS
(Workbook page W71)

15. List three numbers equivalent to each number.

a. 6 mod 12

b. 9 mod 12

16. List three numbers equivalent to each number.

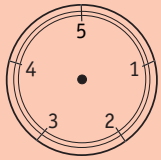


a. 2 mod 10

b. 9 mod 10

c. 0 mod 10

17. List three numbers equivalent to each number.



a. 1 mod 5

b. 3 mod 5

c. 2 mod 5

Another term for "equivalent mod n" is **congruent mod n**. You may have learned the word "congruent" in geometry. Congruent triangles are alike because they have the same size and shape. The symbol "≅" is used in geometry to show that things are congruent. It looks somewhat like the equal sign to remind us that congruent objects are alike, but it is different from "=" because being congruent doesn't really mean being equal.

You can find numbers equivalent to another number by adding multiples of the modulus. For example, 13, 25, 37, and 49 are all equivalent mod 12 to 1 since they are all 1 plus a multiple of 12.

$$1 + 1 \times 12 = 13$$
$$1 + 2 \times 12 = 25$$
$$1 + 3 \times 12 = 37$$
$$1 + 4 \times 12 = 49$$

✎ **Do Problems 15–17 now.**

Reducing mod *n*

When we work mod n, we often use only the numbers from 0 to $n - 1$. If another number comes up, we **reduce mod n**, which means we replace it with the number between 0 and $n - 1$ that is equivalent mod n to it. This is the remainder when we divide by n.

For example, 37 is equivalent mod 12 to the numbers 1, 13, 25, and so on. Of these, the number in the range from 0 to 11 is 1, so reducing 37 mod 12 gives 1.

It is useful to have a notation that means reduce, or find the remainder. We will use mod n without parentheses for this. So 37 mod 12 means the remainder when we divide 37 by 12. Also, when we reduce, we use the equal sign and not the equivalence symbol. We write

$$37 \bmod 12 = 1.$$

Abby thought she understood modular arithmetic, but she wasn't sure she understood reducing.

Jesse said, "Let's work out a problem. Let's reduce $40 \bmod 12$.

"Since we're working mod 12, we need to find the number from 0 to 11 that is equivalent to 40 mod 12. One way to do that is to subtract 12 repeatedly until we get a number between 0 and 11."

$$\begin{array}{r} 40 \\ -\ 12 \\ \hline 28 \\ -\ 12 \\ \hline 16 \\ -\ 12 \\ \hline 4 \end{array}$$

"We stop when we get to a number less than 12, in this case 4."

"Hmm," said Abby, "wouldn't it be faster to subtract a multiple of 12? The greatest multiple of 12 less than 40 is $3 \times 12 = 36$, and $40 - 36 = 4$."

"Yes," said Jesse, "and another way is to divide and find the remainder:

$$12\overline{)40} \quad 3\text{R}4$$

"All these methods lead to the same answer: $40 \bmod 12 = 4$."

Negative numbers work in modular arithmetic, too, if you think about going backward on a clock. For example, $-3 \bmod 12 = 9$. We get this by counting back 3 hours from 12 on a 12-hour clock. Another way is to add 12 until we get a number between 0 and 11:

$$-3 + 12 = 9.$$

✎ **Do Problems 18–24 now.**

PROBLEMS
(Workbook pages W72–W73)

18. Reduce each number.

a. 8 mod 5 **b.** 13 mod 5 **c.** 6 mod 5 **d.** 4 mod 5

19. Reduce each number.

a. 18 mod 12 **b.** 26 mod 12 **c.** 36 mod 12 **d.** 8 mod 12

20. Reduce each number.

a. 8 mod 3 **b.** 13 mod 6 **c.** 16 mod 11 **d.** 22 mod 7

21. Reduce each number.

a. −4 mod 12 **b.** −1 mod 12 **c.** −6 mod 12 **d.** −2 mod 12

22. Reduce each number.

a. −4 mod 10 **b.** −1 mod 10 **c.** −6 mod 10 **d.** −2 mod 10

23. Reduce each number.

a. −3 mod 5 **b.** −1 mod 5 **c.** 8 mod 5 **d.** 7 mod 5

24. Reduce each number.

a. −2 mod 24 **b.** 23 mod 20 **c.** 16 mod 11 **d.** −3 mod 20

CLASS ACTIVITY: The Mod Game

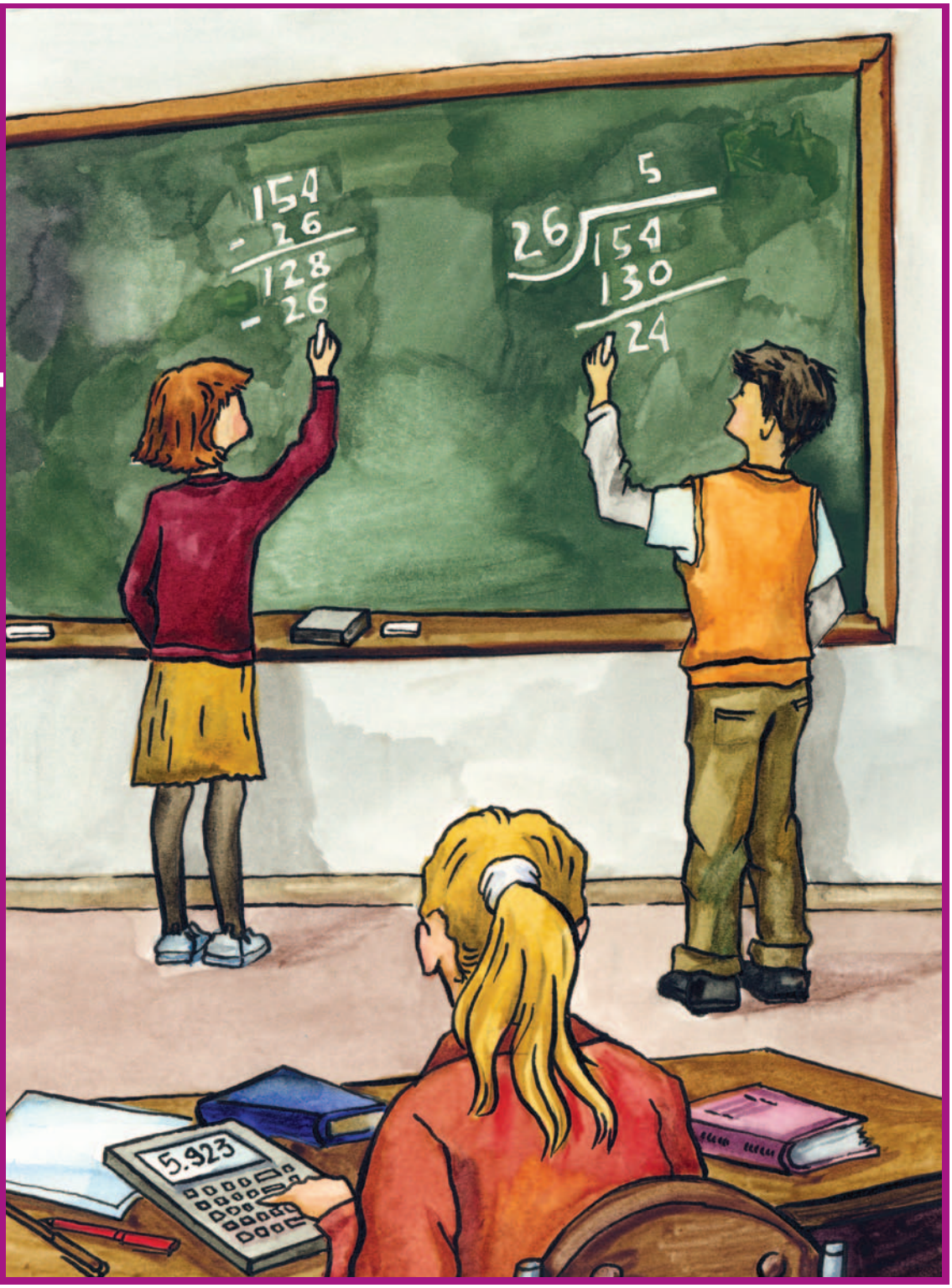
- Divide the class into teams. (Four to seven teams is a good number.) Each team sends a representative to stand in a line facing the class.
- One of the teams chooses a number between 10 and 30. Students in the line "count off" 1, 2, 3,... up to that number.
- The student who calls out the last number wins a point for his team.

  Sample: Suppose there are four teams, T1, T2, T3, and T4. If the number 11 is chosen, then the counting stops at T3 as shown below. Team 3 wins a point.

T1	T2	T3	T4
1	2	3	4
5	6	7	8
9	10	11	

- Another team chooses a number, and the counting is repeated.
- After you have played for a while, divide the class into a different number of teams and play again.

Chapter 12



Applications of Modular Arithmetic

"I think we've been using modular arithmetic in our ciphers without knowing it," said Tim.

"I think you're right," agreed Lilah. "When we used Caesar ciphers, we wrote the letters as numbers and then added to encrypt. But if the sums were greater than 25, we substituted 0 for 26, 1 for 27, and so on. That's just like reducing mod 26."

Tim and Lilah were right. Using modular arithmetic, they could write

$26 \bmod 26 = 0$
$27 \bmod 26 = 1$
$28 \bmod 26 = 2$, and so on.

To reduce a negative number mod 26, you add 26 to get a number in the range 0 to 25.

$-1 \bmod 26 = 25$
$-2 \bmod 26 = 24$
$-3 \bmod 26 = 23$, and so on.

✎ **Do Problems 1–3 now.**

PROBLEMS
(Workbook page W75)

1. Reduce the following numbers mod 26:

a. 29 **b.** 33 **c.** 12
d. 40 **e.** −4 **f.** 52
g. −10 **h.** −7

Use multiplication to make a cipher. The rule for encrypting is given in the table below.

2. Encrypt the name "Jack" using the times-5 cipher. The first two letters are done for you.

Times-5 Cipher	J	a	c	k
change letters to numbers (use cipher strip)	9	0		
multiply by 5	45	0		
reduce mod 26	19	0		
change numbers to letters	T	A		

PROBLEMS
(Workbook page W75)

3. Encrypt "cryptography" using the times-3 cipher as described in the table below. The first two letters are done for you.

Times-3 Cipher	c	r	y	p	t	o	g	r	a	p	h	y
change letters to numbers (use cipher strip)	2	17										
multiply by 3	6	51										
reduce mod 26	6	25										
change numbers to letters	G	Z										

Tim and his friends decided to use what they called the times-11 cipher. They changed letters to numbers, multiplied by 11, and reduced mod 26. But multiplying by 11 gave some pretty large numbers. They had to figure out how to reduce these numbers mod 26. For example, to encrypt the letter **m**, which corresponds to 14, they computed 11 × 14 = 154. Then they needed to reduce 154 mod 26. How would you solve this problem?

Dan decided to subtract 26 over and over (*left*), until he got an answer less than 26.

```
154
− 26
128
− 26
102
− 26
 76
− 26
 50
− 26
 24
```

154 mod 26 = 24.

Jenny decided to divide by 26, since the remainder is the desired answer. In this method, 154 ÷ 26 = 5 R 24, so 154 mod 26 = 24. You can divide using long division or using a calculator. (For tips on how to use a calculator to find the remainder, see the next section.)

Lilah decided to subtract a multiple of 26 from 154. Multiples of 26 are 26, 52, 78, 104, 130, 156, ... In this problem, 130 is the largest multiple you can subtract from 154. Since 154 − 130 = 24, 154 mod 26 = 24. (If you subtract a smaller multiple of 26, for example, 104 instead of 130, you would have to keep subtracting until you get a number less than 26.)

Jesse decided to estimate the number of times 26 goes into 154 and subtract that many 26s from 154. He guessed 26 goes into 154 about 5 times, since he knew that 5 × 30 is 150. He calculated 5 × 26 = 130 and subtracted this from 154. If his guess had been too low, he could have subtracted more until his answer was less than 26.

All of their methods gave the same answer, 154 mod 26 = 24, which corresponds to the letter **Y**. In the times-11 cipher, **m** is encrypted as **Y**.

✎ **Do Problems 4 and 5 now.**

Using a Calculator to Find Remainders

To find 154 mod 26, Tim and Abby wanted to divide and find the remainder. They could do this using long division, but instead they chose to use their calculators. With their calculators, they found that

$$154 \div 26 = 5.9230769$$

The calculator expressed the remainder as a decimal, but they wanted it expressed as a whole number. Tim and Abby used two different methods to find the whole number remainder from the decimal remainder.

Tim thought, "The calculator answer tells that there are 5 groups of 26 in 154, plus some left over. (The leftover amount is the decimal 0.9230769.) The 5 groups of 26 are 5 × 26 = 130. This leaves 154 – 130 = 24 left over. Therefore 154 ÷ 26 = 5 R 24. So 154 mod 26 = 24."

PROBLEMS
(Workbook page W76)

4. Reduce each number.
   - **a.** 175 mod 26
   - **b.** 106 mod 26
   - **c.** 78 mod 26
   - **d.** 150 mod 26
5. Reduce each number. (Hint: Try subtracting multiples of 26 such as 10 × 26 = 260.)
   - **a.** 586 mod 26
   - **b.** 792 mod 26
   - **c.** 541 mod 26
   - **d.** 364 mod 26

Abby thought, "The calculator answer is 5.9230769. To get the decimal remainder, I'll subtract off the 5." (This is better than retyping the decimal part, since it saves the extra places stored in the calculator that help prevent round-off error.)

$$5.9230769 - 5 = 0.9230769$$

"I know that a decimal remainder is computed by dividing the remainder R by the divisor. In this case, the divisor is 26, so

$$\frac{R}{26} = 0.9230769.$$

"To solve this, I'll multiply both sides by 26:

$$26 \times \frac{R}{26} = 0.9230769 \times 26.$$

"This gives

$$R = 24."$$

Abby discovered that when she found remainders this way she didn't always get whole number answers for R. She knew that was because of calculator round-off during division. This didn't happen often, but when it did, she adjusted her answer by rounding it to the nearest whole number.

✎ **Do Problems 6–8 now.**

PROBLEMS
(Workbook pages W76–W77)

6. Use a calculator to help you reduce the following.

- **a.** 254 mod 24
- **b.** 500 mod 5
- **c.** 827 mod 26
- **d.** 1500 mod 26
- **e.** 700 mod 9
- **f.** 120 mod 11

7. Reduce each number.

- **a.** 500 mod 7
- **b.** 1000 mod 24
- **c.** 25,000 mod 5280
- **d.** 10,000 mod 365

8. Choose one of the numbers you reduced in Problem 6. Write how you would explain to a friend the way you reduced your number.

Shortcut for Multiplying mod 26

Tim wanted to encrypt his name using the times-11 cipher. He started to multiply by 11 and reduce modulo 26, but working with these numbers turned out to be very tedious. For example, to encrypt **Y**, he multiplied $24 \times 11 = 264$. To reduce this he could divide 264 by 26 and find the remainder, but this was more work than he wanted to do. He thought of a shorter way: He realized that $24 \equiv -2 \pmod{26}$. Multiplying by congruent numbers gives the same answer in modular arithmetic, so

$$\begin{aligned} 11 \times 24 &\equiv 11 \times (-2) \pmod{26} \\ &\equiv -22 \pmod{26} \\ &\equiv 4 \pmod{26}. \end{aligned}$$

✎ **Do Problem 9 now.**

Calendar Applications for Modular Arithmetic

The kids' teacher told them that modular arithmetic is useful for solving problems that involve cycles, such as calendar problems. She asked them, "If today is Sunday, what day of the week will it be in 50 days?"

Suppose you think of Sunday as Day 0, Monday as Day 1, etc. Then the numbers 0 to 6 represent the seven days of the week. Day 7 is Sunday again. Every day whose number is 0 mod 7 is Sunday. Every day whose number is 1 mod 7 is Monday, and so on. Since $50 \bmod 7 = 1$ (why?), the fiftieth day is Monday.

✎ **Do Problems 10–15 now.**

★ TIP: Tim's Shortcut for Multiplying modulo 26

If the multiplication is messy, subtract 26 to get a number that (1) is congruent mod 26 to your number and (2) might be easier to work with.

PROBLEMS (Workbook page W77)

9. Encrypt "trick," using the times-11 cipher. Use Tim's shortcut when it makes your work easier.

Times-11 Cipher	t	r	i	c	k
change letters to numbers					
multiply by 11					
reduce mod 26					
change numbers to letters					

PROBLEMS
(Workbook page W78–W80)

10. Astronauts left on a Sunday for a mission into space. On what day of the week would they return if they were gone for

a. 4 days? **b.** 15 days? **c.** 100 days? **d.** 1000 days?

11. If today is Wednesday, what day of the week will it be in

a. 3 days? **b.** 75 days? **c.** 300 days?

Leap Years. There are 365 days in a year, except for leap years. In a leap year, an extra day (February 29) is added, making 366 days. Leap years occur in years divisible by 4, except at the beginning of some centuries. Years that begin new centuries are not leap years unless they are divisible by 400. So 1900 was not a leap year but 2000 was.

12. **a.** 2004 was a leap year. What are the next two leap years?

b. Which of the following century years are leap years?
1800, 2100, 2400

c. Which of the following years were leap years?
1996, 1776, 1890

13. If the Fourth of July is on Tuesday this year, on what day of the week will it be next year? (Assume that next year is not a leap year.) Explain how you got your answer.

14. **a.** What is today's day and date?

b. What day of the week will it be on today's date next year? Your answer will depend on whether or not a leap year is involved. Explain how you got your answer.

15. **a.** On what day and date will your next birthday be? (You may use a calendar.)

b. On what day of the week will your twenty-first birthday be? Answer without using a calendar. Don't forget about leap years. Explain how you got your answer.

DO YOU KNOW?
Non-Secret Codes

Not all codes are secret codes. For example, the International Standard Book Numbers (ISBNs) on books and Universal Product Codes (UPCs) on other products are designed to store information in a form easily understood by a computer. But this information is not meant to be secret.

Codes often store more information than just the name of the product. For books published before 2007, the ISBN is a 10-digit number divided into four parts. The first part tells the country or language area in which a book is published (0 or 1 represents English-speaking countries such as the United States, the United Kingdom, Australia, etc.). The second part identifies the publisher, and the third part is assigned by the publisher to identify the book itself. The last part, the tenth digit, is a special digit, called the check digit. It can help to check whether a mistake is made in typing or sending the number. It is not surprising that mistakes are sometimes made, but it might surprise you that the codes are designed to detect mistakes.

After the first nine digits of a book's ISBN are assigned, the check digit is chosen so that the sum of 10 times the first digit, plus 9 times the second digit, plus eight times the third, and so on, up to 1 times the tenth digit is equivalent to 0 mod 11. In other words, that sum is a multiple of 11. The number on the back of this book is ISBN 1-56881-223-X. The X stands for 10 (the check digit must be only one digit, so X is used in place of 10). You can check that

$$(10 \times 1) + (9 \times 5) + (8 \times 6) + (7 \times 8) + (6 \times 8) + (5 \times 1) + (4 \times 2) + (3 \times 2) + (2 \times 3) + (1 \times 10) = 242 \equiv 0 \bmod 11.$$

CONTINUED ON NEXT PAGE >

DO YOU KNOW? (CONTINUED)
Non-Secret Codes

Suppose someone tried to order this book but made a mistake and typed ISBN 1-56881-223-6 instead. The computer would calculate

$$(10 \times 1) + (9 \times 5) + (8 \times 6) + (7 \times 8) + (6 \times 8) + (5 \times 1) + (4 \times 2) + (3 \times 2) + (2 \times 3) + (1 \times 6) = 238.$$

Since this is not a multiple of 11, the computer would warn that the number typed is incorrect — it couldn't possibly be the ISBN for a book.

Beginning in 2007, the ISBNs will be 13-digit numbers. This is because 10-digit numbers are running out. A three-digit prefix will be added to the front, the way area codes are added to phone numbers. Future printings of this book will have 978 added to the front, and the check digit will change. Instead of multiplying the first digit by 10, the second by 9, and so on, the new check digit will be determined by multiplying the first digit by 1, the second by 3, the third by 1, the fourth by 3, and so on, alternating 1 and 3. The check digit will be the number needed to make the sum a multiple of 10 (instead of 11, as in the old scheme). Thus the number of this book will become ISBN 978-1-56881-223-6 because

$$(1 \times 9) + (3 \times 7) + (1 \times 8) + (3 \times 1) + (1 \times 5) + (3 \times 6) + (1 \times 8) + (3 \times 8) + (1 \times 1) + (3 \times 2) + (1 \times 2) + (3 \times 3) + (1 \times 6) = 120,$$

which is a multiple of 10.

The ISBN code can detect errors, but some codes are so sophisticated that they can do more than that. Some codes can actually correct the errors. There is an entire field of mathematics devoted to the study of error-correcting codes.

Modular Arithmetic: Reducing mod *m*

Definition: The expression $a \equiv b \pmod{m}$, which is read: "*a* is congruent to *b* mod *m*" means that

$m \mid a - b$, read "*m divides* $a - b$

which is the same as

$a - b$ is a multiple of m

or the same as

m is a factor of $a - b$.

or the same as

a and *b* have the same remainder when divided by *m*

Make sure you can explain why these four statements all say the same thing and how each relates to the mod spiral and clock arithmetic. Why is the symbol ≡ used instead of an equal sign, = ?

Examples: Which statements are true and which are <u>not</u> true? Explain your reasoning for each example. Try for the easiest way to see it. Two are done.

$27 \equiv 53 \pmod{26}$ $81 \equiv 807 \pmod{8}$ $138 \equiv 118 \pmod{26}$

true: same remainder when divided by 26

$159 \equiv 129 \pmod{30}$ $173 \equiv 121 \pmod{26}$ $77 \equiv 140 \pmod{7}$

true: the difference of the two is a multiple of 30

Definition: *a* mod *m* means the remainder when *a* is divided by *m*.

We call the number *a* mod *m* "*a* reduced mod *m*." The remainder is always between 0 and $m - 1$, so *a* mod *m* is always a number between 0 and $m - 1$

Example: The expression "37 mod 26" means the remainder when dividing 37 by 26. In this case we write 37 mod 26 = 11. Note: It is also true that 37 = 11 (mod 26) and, as well, 11 = 37 (mod 26). It is not true that 11 mod 26 = 37. The right hand side must be a remainder. Explain why each of the following statements is true.

53 mod 26 = 1 181 mod 8 = 5

true: $53 = 2 \cdot 26 + 1$

149 mod 30 = -1 173 mod 26 = 17

false: even though $149 \equiv -1 \pmod{30}$.

Why is the equal sign = used in these last examples instead of symbol ≡?

Notice: $a \equiv b \pmod{m}$ only when $a \bmod m = b \bmod m$

Negative Numbers can be useful as well. Because we were careful when we stated the Division Algorithm we know how to reduce negative numbers.

Examples: Which statements are true and which are <u>not</u> true? Explain your reasoning for each example.

-1 mod 26 = 25
true: -1 = -1·26 + 25

-81 ≡ 807 (mod 8)

-18 ≡ 44 (mod 26)

-24 ≡ 24 (mod 26)
false: -24 = 26(-1)+2
so -24 is equivalent to 2

-173 ≡ 121 (mod 26)

-77 ≡ 140 (mod 7)

Modular Arithmetic: Rules

When doing arithmetic in modular arithmetic the fundamental rule is that when adding, subtracting, and multiplying, one can reduce after any step and, as long as you reduce at the very end, you will get the same answer as you would if you had reduced after other steps or never reduced at all until the very end. In fact, when adding, subtraction, multiplying you can replace a number by any other number that is congruent to it! **Warning**: As we will see later, the same is not true about division.

Example 1: Here are two ways to compute (15 x 2) + 24 mod 26

$$\begin{aligned}(15 \text{ X } 2) + 24 &\equiv 30 + 24 \pmod{26}\\ &\equiv 54 \pmod{26}\\ &\equiv 2 \pmod{26}\end{aligned}$$

$$\begin{aligned}(15 \text{ X } 2) + 24 &\equiv 30 + 24 \pmod{26}\\ &\equiv 4 + 24 \pmod{26}\\ &\equiv 28 \pmod{26}\\ &\equiv 2 \pmod{26}\end{aligned}$$

Example 2: This one is fun:

$$\begin{aligned}23 \text{ x } 25 &\equiv 23 \text{ x } (-1) \pmod{26} \quad \text{because } 25 \equiv -1 \pmod{26} \text{ !!}\\ &\equiv -23 \pmod{26} \quad \text{because } -23 - 3 = -1 \text{ x } 26\\ &\equiv 3 \pmod{26}\end{aligned}$$

But the best example is seen when computing a power. Because exponentials grow so fast it is easy to run out of calculator digits. Too avoid this just reduce after a lower power and resume.

Example 3: Compute 2^{20}.

$2^{20} = 2^5 \cdot 2^5 \cdot 2^5 \cdot 2^5 = 32^4 \equiv 6^4 \equiv 6^2 \cdot 6^2 \equiv 36 \cdot 36 \equiv 10 \cdot 10 \equiv 100 \equiv 22 \bmod 26$

The following two facts sum up the rules for working with addition and multiplication: We can add the same number to both sides of a congruence equation. We can multiply both sides of a congruence equation by the same number. The statement remains true if it started true and remains false if it started false.

Rule 1 If $a \equiv b \pmod{m}$, then $a+c \equiv b+c \pmod{m}$ for any integer c.
It is easy to see why this Rule is true: the difference between $a+c$ and $b+c$ is the same as the difference between a and b. a is equivalent to b mod m exactly when $a+c$ is equivalent to $b+c$ mod m.

Rule 2 If $a \equiv b \pmod{m}$, then $a \cdot c \equiv b \cdot c \pmod{m}$ for any integer c.
Why? Easy. If $a - b$ is a multiple of m then so is $(a - b) \cdot c = a \cdot c - b \cdot c$
Notice, however, that if $(a - b) \cdot c$ is a multiple of m we can not conclude that $a - b$ is also a multiple of m. Why not?

Congruence Equations: Like regular arithmetic, the rules on the preceding page are what we need to solve equations:

1. Explain how to use these two rules to find the reduced solutions to the following equations:

$x - 7 \equiv 22 \pmod{26}$
add 7 to both sides
solution: x mod 26 ≡ 3

$7 \equiv x - 2 \pmod{12}$

$x + 7 \equiv 3 \pmod{13}$

$47 \equiv 2 - x \pmod{53}$

Instead of adding the same number to both sides I can, in fact, add two different numbers as long as they are equivalent.

Rule 3 If $a \equiv b \pmod{m}$ and if $c \equiv d \pmod{m}$, then $a+c \equiv b+d \pmod{m}$

We can see why in two steps. First, we know that $a+c \equiv b+c \pmod{m}$ by adding c to the first congruence we are given. Second, we add b to the second congruence, so we know that $b+c \equiv b+d \pmod{m}$. We have two expressions that are both congruent to $b+c$ so we must conclude that they are also congruent to each other, or $a+c \equiv b+d \pmod{m}$

Rule 4 If $a \equiv b \pmod{m}$ and if $c \equiv d \pmod{m}$, then $a \cdot c \equiv b \cdot d \pmod{m}$ for any integers c and d as long as $c \equiv d \pmod{m}$.

2. Provide the explanation for **Rule 4**:

Modular Arithmetic: More Congruence Equations

Even simple equations in modular arithmetic may have more than one solution or no solutions.

Example 1: $2x \equiv 8 \pmod{26}$

What happens if we cancel a factor of two from both sides of the equation? We get $x \equiv 4 \pmod{26}$. Although it is true that $x = 4$, is a solution to this equation, it is also true that $x = 17$ (not congruent to 4 (mod 26)) is another solution. To see this multiply 2 times 17 to get 34. 34 reduces to 8 mod 26. Therefore, cancelling a factor of 2 from both sides of the equation is a bad strategy unless you are very sure you know what you are doing and have an additional strategy to find other solutions.

Example 2: $2x \equiv 7 \pmod{26}$

This equation has no solution because every even number reduces mod 26 to an even number. This is because 26 is even so subtracting or adding multiples of 26 to an even number results in an even number.

Example 3: $3x \equiv 8 \pmod{26}$

This example is very different. We know from our work with multiplicative ciphers that we can solve this equation: multiply both sides by the multiplicative inverse of 3 mod 26. Recall that $3^{-1} \bmod 26 \equiv 9$. So

$9\cdot(3x) \equiv 9\cdot 8 \pmod{26}$	multiply both sides by 9
$(9\cdot 3)\cdot x \equiv 9\cdot 8 \pmod{26}$	apply associative rule
$27\cdot x \equiv 72 \pmod{26}$	evaluate: $9\cdot 3 = 27$
$1\cdot x \equiv 72 \pmod{26}$	reduce: 27 mod 26 = 1
$x \equiv 72 \pmod{26}$	1 is multiplicative identity
$x = 20 \pmod{26}$	reduce: 72 mod 26 = 20

The solution then is any x, such that $x \bmod 26 = 20$.

Solve the following congruence equations. Write your final answer in the form $x \bmod m = a$ Determine whether or not the equation has more than one reduced solution, like **Example 1**. Or no solutions, like **Example 2**. Or one reduced solution, like **Example 3**.

$2x \equiv 1 \pmod{6}$ $2x \equiv 4 \pmod{6}$ $5x \equiv 2 \pmod{6}$

$29x \equiv 1 \pmod{83}$ $29x \equiv 17 \pmod{83}$ $91x \equiv 23 \pmod{136}$

$132x \equiv 33 \pmod{253}$ $132x \equiv 25 \pmod{253}$

Modular Arithmetic: Common Factors

Division: Division is trickier. In general, division works differently in modular arithmetic because we don't have fractions. If the divisor is a factor of the dividend, we can give meaning to division. However, removing a common factor from two equivalent numbers may result in two numbers that are NOT equivalent.

Example:

$16 \equiv 42 \pmod{26}$ is a true statement, but $8 \equiv 21 \pmod{26}$ is NOT true.

We cannot cancel a factor of 2 from both sides of the original congruence. We cannot divide both sides of a true congruence statement by the same number and be guaranteed the result is also true.

1. For which of the following equivalent numbers (in the given mod) can you factor out a common factor and still have to numbers that are equivalent.

$12 \equiv 90 \pmod{26}$ $3 \equiv 33 \pmod{10}$

$28 \equiv 210 \pmod{26}$ $15 \equiv 5 \pmod{10}$

2. Find four more examples using different mods. Find two where you can cancel a common factor and two where you cannot.

The final rule we study tells us when it is possible to cancel common factors from two equivalent numbers and still have equivalent numbers:

Rule 6 If $a \cdot c \equiv b \cdot c \pmod{m}$ and if gcd $(c,m) = 1$, then $a \equiv b \pmod{m}$.

Why is this true? Consider $a \cdot c - b \cdot c = (a - b) \cdot c$. Since c and m have no factors in common, all the common factors of $(a - b) \cdot c$ and m must be factors of $a - b$. Hence m divides $a \cdot c - b \cdot c$ assures that m also divides $a - b$ or $a \equiv b \pmod{m}$.

Modular Arithmetic: Divisibility Rules Explained

One consequence of these rules is another rule that we have already seen can be very useful:

Rule 7 If $a \equiv b \pmod{m}$, then $a^c \equiv b^c \pmod{m}$

We can use this rule to help us understand why the various divisibity tests work the way they do.

Divisibility by 3: Let $m = 3$. Notice that $10 \equiv 1 \pmod{m}$. So, by Rule 7, $10^n \equiv 1^n \equiv 1 \pmod{m}$ for any integer n. What does that mean about divisibility by 3. Consider a number, like 471

$471 = 4 \cdot 10^2 + 7 \cdot 10^1 + 1 \cdot 10^0 \equiv 4 \cdot 1 + 7 \cdot 1 + 1 \cdot 1 \equiv 4 + 7 + 1 \pmod{m}$

So the number 471 is divisible by 3 exactly when the some of it's digits, 4+7+1, is divisible by 3. 471 is divisible by 3 because 12 is divisible by 3. In short we have:

A number is divisible by 3 exactly when the sum of the digits is divisible by 3

Divisibility by 8 Now consider $m = 8$. As above, we will reduce all powers of 10:

$10 \bmod 8 = 2$
$10^2 \bmod 8 = 2^2 \bmod 8 = 4$
$10^3 \bmod 8 = 2^3 \bmod 8 = 0$
$10^4 \bmod 8 = 10^3 \cdot 10^1 \bmod 8 = 0$
$10^5 \bmod 8 = 10^4 \cdot 10^1 \bmod 8 = 0$, and so on $10^n \bmod 8 = 0$, for $n > 2$.

Now consider a number like 4766: $4766 = 4 \cdot 10^3 + 766 \bmod 8 = 0 + 766 \bmod 8$, so 4766 is divisible by 8 exactly when 766 is divisible by 8. Since 766 is not divisible by 8 neither is 4766. But 5,468,808 is divisible by 8 because 808 is.

A number is divisible by 8 exactly when the last three digits is divisible by 8.

1. Explain a divisibility by 9 rule using mod 9 arithmetic

2. Explain a divisibility by 4 rule using mod 4 arithmetic

Modular Arithmetic: Finding Multiplicative Inverses

We want to solve modular equations that look like:

$3x \equiv 1 \pmod{26}$

This means find a multiple of 3 that is equal to 1 + a multiple of 26 OR
$3x = 1 + 26m$ OR
$3x - 26m = 1$ OR
$3x + 26y = 1$ $(y=-m)$

Find a values for (x and y) that solve this equation.
Find the value of x reduced mod 26 that is the inverse of 3 mod 26.

Because the extended algorithm works for any numbers we can find the multiplicative of lots of numbers in different mods.

And we have a way of finding out when a number will have a multiplicative inverse.

Please notice the middle schoolers can find the inverse mod 26 in straight-forward tedious methods. They could try other mods and other inverses but it would be tedious without the extended Euclidean algorith
m.

4-digit Multiplicative Cipher: Mod 10000

To further challenge those who would try to crack our cipher, we next consider enlarging our alphabet by taking two letters at a time. To do this first change the plaintext letters to numbers, then lump the numbers together in groups of four digits. To avoid ambiguity, it is important to always include the leading zero. Our new alphabet consists of four digit numbers.

With this procedure, numbers may be as large as 9999. So we will work mod 10000.

Encrypt by multiplying by 37 mod 10000:

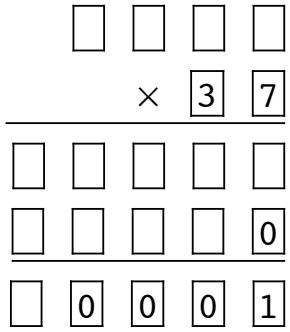
Example: **your name**:

	s a	u n	d e	r s
convert to numbers and lump:	1800	2013	0304	1718
multiply by 37 and reduce:	6600	4481	1248	3566

\

Decrypting: What is the multiplicative inverse of 37 mod 10000? What number times 37 is congruent to 1 mod 10000.. Find a number such that when you multiply it by 37 the last four digits are 0001.

In a few pages we will learn, the efficient way to proceed, but this can be a fun place-value problem, so let's try a simple-minded, tedious approach using the standard multiplication algorithm. It's similar to sideways arithmetic and starts looking like this:
Can you fill in the blanks with digits 1 – 9 to complete the problem and find the inverse mod 100000?



(There may be one more digits to the left in the answer)
So 2973 is the multiplicative inverse of 37 mod 10000. So to decrypt we first multiply by 2973 and then reduce mod 10000

Example: Decrypting 6600 4481 1248 3566
6600 x 2973 = 19621800 ≡ 1800 mod 10000

3. To check your understanding of how this works, finish decrypting 6600 4481 1248 3566

4. Exchange encrypted names with someone and decrypt.

5. Decrypt this message that was encrypted by lumping letters by twos and multiplying the resulting four digits numbers by 37 mod 10000. You may want to work together to get all this multiplying and reducing done:

I f	y o	u r	e a	d a	l o	t o	f b	o o	k s	y o
0805	2414	2017	0400	0300	1114	1914	0501	1414	1018	2414
9785	9318	4629	4800	1100	1218	0818	8537	2318	7666	9318

u a	r e	c o	n s	i d	e r	e d	w e	l l	r e	a d
2000	1704	0214	1318	0803	0417	0403	2204	1111	1704	0003
4000	3048	7918	8766	9711	5429	4911	1548	1107	3048	0111

b u	t i	f y	o u	w a	t c	h a	l o	t o	f t	v y
0120	1908	0524	1420	2200	1902	0700	1114	1914	0519	2124
4440	0596	9388	2540	1000	0374	5900	1218	0818	9203	8588

o u	r e	n o	t c	o n	s i	d e	r e	d w	e l	l v
1420	1704	1314	1902	1413	1808	0304	1704	0322	0411	1121
2540	3048	8618	0374	2281	6896	1248	3048	1914	5207	1477

i e	w e	d l	i l	y t	o m	l i	n a
0804	2204	0311	0811	2419	1412	1108	1300
9748	1548	1507	0007	9503	2244	0996	8100

4-digit Multiplicative Cipher: Mod 9999

Actually, lumping together produces numbers that are no larger than 2525. Which means that any modulus greater than 2525 could be used for a multiplicative cipher. The range of the cipher may not be the same as the domain but that doesn't stop the cipher from working both for encryption and decryption.

Here is a message that has been encrypted by multiplying by 25 mod 9999:

0076 0055 0475 0352 2703 5329 5478 0375 2604 7503 2504

7704 5328 2851 2779 0127 0101 8000 5000 7704 5328 0452

7702 2601 0477 5104 7627 2852 7826 7600 5105 0006

Example of encryption: your name encrypted this way:

```
 s a  u n  d e  r s
1800 2013 0304 1718
5004 0330 7600 2954
```

\

What is the multiplicative inverse of 25 mod 9999? What number times 25 is congruent to 1 mod 9999. Well, that's easy! Something times 25 that gives me 10000 is 400.
(or solve: 25X = 9999Y+1)

400 is the multiplicative inverse of 25 mod 9999. So multiply by 400 (and reduce of course) to decrypt.

Example: Decrypting 5004 0330 7600 2954

5004 x 400 = 2001600 = 2000000 + 1600 = 200*9999 +200 +1600 ≡ 1800 mod 9999

Finish the decryption.

6. Exchange encrypted names with someone and decrypt.

7. Decrypt the message at the top of this page:

```
 e d  u c  a t  i o  n i  s n  o t  a p  r e  p a  r a  t i  o n
0403 2002 0019 0814 1308 1813 1419 0015 1704 1500 1700 1908 1413
 f o  r l  i f  e e  d u  c a  t I  o n  i s  l i  f e  i t  s e
0514 1711 0805 0404 0320 0200 1908 1413 0818 1108 0504 0819 1804
l f  J o  h n  D e  w e  y a
1105 0914 0713 0304 2204 2400
```

8. What other numbers make good multiplicative keys mod 9999?

4-digit Multiplicative Cipher: Finding Inverses

Here is a review of the efficient, elegant way to find the inverse: using the extended Euclidean algorithm.

Example 1: To find the multiplicative inverse of 37 mod 10000, we have to find a number (call it X) such that when we multiply that number by 37 we get 1 mod 10000. Or when we multiply that number by 37 we get a multiple of 10000 plus 1 (say 10000·Y + 1). So we can write an equation:

37·X = 10000·Y + 1 or 37·X - 10000·Y = 1 or 37·X + 10000·(- Y) = 1

Use the Extended Euclidean Algorithm or find the solution on your calculator.

[**More concerns about negative numbers**: Do not let the –Y worry you. Just solve the Diophantine equation as usual. At the last minute you can change the sign of the answer. That is you find –Y so Y is the opposite of the answer. Another reason not to worry, is that for our problem we really don't care what Y is what we are looking for is X]

Example 2: To find the multiplicative inverse of 25 mod 9999, we have to find a number (call it X) such that when we multiply that number by 25 we get 1 mod 9999. Or when we multiply that number by 25 we get a multiple of 9999 plus 1. So we can write an equation:

25·X = 9999·Y + 1 or 25·X - 9999·Y = 1 or 25·X + 10000·(- Y) = 1

Use the Extended Euclidean Algorithm or find the solution on your calculator.

Procedure: To find the multiplicative inverse of a number, A mod M, we have to find a number (call it X) such that when we multiply that number by A we get 1 mod M. Or when we multiply that number by A we get a multiple of M plus 1.

A·X = M·Y + 1 or A·X - M·Y = 1 or A·X - M·Y = 1

You try it: The answer to this riddle was encrypted by multiplying by 77 mod 3000. What's the answer?

RIDDLE: How do trees get on the internet?
ANSWER: 2839 2648 1778 1816 1100

T h e y l o g i n.
1907 0424 1114 0608 1300

4-digit Multiplicative Cipher: Project

THINK OF A RIDDLE WITH A SHORT ANSWER.
THINK OF A MODULUS AND A GOOD MULTIPLICTIVE KEY
ENCRYPT THE ANSWER WITH FOUR DIGIT MULTIPLICATIVE CODE

Think of a multiplicative key k with modulus 2600. Make sure it's a good key.

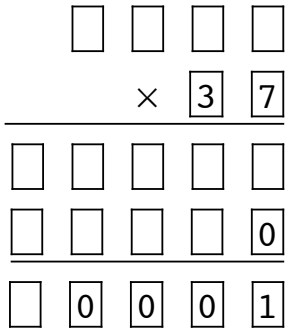
Play cipher tag. Talk about problems. Use WolframAlpha to find inverses

http://www.wolframalpha.com

In your own words: What makes a good multiplicative key mod 2600

Presentation Idea

Make up more problems like this one that we solved at the beginning of this chapter. This can be a fun place-value problem, it's similar to sideways arithmetic and starts looking like this:



2 9 7 3
3 7
2 0 8 1 1
8 9 1 9 0
0 0 0 1

(There may be one more digits to the left in the answer)
Find the digits that fill in the blanks to make the answer come out as shown.

Make some problems like this one that are simpler but would still be a challenge for middle school students. **Challenge for you**: Make a problem that has more than one correct answer.

Teaching: Prime Numbers

Your group will be assigned a project to teach to the class. Each project should include the following components. You will be allowed 15 minutes of class time.

1. Research: You should include information that extends beyond what you find in the Cryptoclub Book. Resources: Your first resource should be the CryptoClub book, Chapter 16. The internet should be more than enough to find further information.

2. Class activity: You should contact an activity in class to help us all understand better what your project is about. Activities from the book need to be extended to keep the interest of a college class. Everyone will have our class made list of primes less than 10,000. Use this resource to work with prime numbers that are larger than the ones expected to be used by children. For sources of activities, please consult with Prof. Saunders. Send an email or make an appointment to meet in her office.

3. Homework assignment: You need to collect some work to evaluate what the class learned from your presentation. Formulate one or two problems for the class to do as homework. I expect to test this material on the final exam.

PROJECT	GROUP
Testing primes (pages 155-160 in CryptoClub)	
Counting primes (pages 161-162 in CryptoClub)	
Mersenne Prime Search	
Twin Primes	
The Goldbach Conjecture	
Sophie Germaine Primes	
n^2-n+41 and other formulas for prime numbers	

Due dates:

Proposal
Presentation to Gail
Presentation to class.
Problems for class

Chapter 16

Finding Prime Numbers

The Cryptoclub had a planning meeting to talk about what to work on next.

"I think we should learn something more modern," said Jesse. "The ciphers we have worked with so far have been around for centuries."

"I agree," said Becky. "They were fun to learn about, but ciphers have to be more complicated today. Computers make the old ones too easy to crack."

Fortunately, Tim had been reading a bit about modern-day ciphers. "Well, the RSA cipher is probably the most widely known modern cipher," explained Tim. "It is named after Ronald Rivest, Adi Shamir, and Leonard Adleman who invented it in 1977. It uses prime numbers—very large prime numbers—and it involves raising numbers to powers in modular arithmetic."

"Do we know enough math to learn about RSA?" wondered Jenny.

"I think we ought to review what we know about prime numbers," Tim said. "Especially larger prime numbers than we usually work with. Then we ought to practice raising numbers to powers in modular arithmetic. That is trickier than you might think, even with a calculator."

"OK, that sounds like plenty to do for the next few meetings," said Jenny. "When we're ready, we'll take a look at the details of RSA. Let's start with prime numbers."

The club members remembered some things about primes, and they knew some small prime numbers like 2 and 3, but Tim explained that to use RSA they would have to be able to find larger primes.

"I can't always tell whether a number is prime," said Peter. "I've been tricked by numbers that look prime but are not. My favorite example is 91. It looks prime to me and to most people I ask, but it turns out not to be prime: $91 = 7 \times 13$."

"You can tell whether a number is prime by testing whether it is divisible by any of the numbers that are smaller than it," said Becky.

"Sure, but that can be a lot of work if the number is large," said Peter. "Take 113, for example. It looks prime. But do I really have to test all the numbers up to 113 to find whether it has any factors besides itself and 1?"

"Why don't we check a few numbers and see what happens?" said Jenny. She got out her calculator.

> "113 is not divisible by 2 since $113 \div 2$ is not a whole number. Besides, it isn't an even number so it can't be divisible by 2.
>
> "113 is not divisible by 3 since $113 \div 3$ is not a whole number. Also, the sum of its digits is not divisible by 3.
>
> "113 is not divisible by 4 since…."

"Wait—we don't have to test 4," Peter interrupted. "If 113 were divisible by 4, then it also would be divisible by 2. So we don't even have to check 4."

Jenny continued:

> "113 is not divisible by 5 since $113 \div 5$ isn't a whole number. Besides, multiples of 5 always end with 0 or 5, so that's another reason I know 113 cannot be a multiple of 5.
>
> "We don't have to check 6. If 113 were divisible by 6, it would have been divisible by 2 and 3. We already know it isn't."

"I see," Peter observed. "We only have to check the prime numbers to see if they divide 113. If 113 isn't divisible by a prime then it couldn't

be divisible by any multiple of that prime either. That is a pretty good shortcut.

"So to check whether 113 is prime," Peter continued, "Let's test every prime number less than 113. The next prime is 7."

"113 is not divisible by 7 since 113 ÷ 7 is not a whole number."

"Wait," said Jenny. "Let's think before we do anymore calculations." Both Jenny and Peter had learned that thinking first often helps to cut the work. They liked math, but they liked to avoid extra work even more.

"The next prime is 11," Jenny thought out loud. "And $11 \times 11 = 121$, which is greater than 113."

"If the product of two numbers is 113," reasoned Peter, "at least one of them must be less than 11. If they both were 11 or more, then their product would be 121 or more."

"But we already showed that none of the primes less than 11 is a factor of 113," said Jenny. "So we don't have to check anything else. It must be that 113 is prime."

"To find that 113 is a prime number, we only had to check four primes. That was pretty quick." Peter was impressed. "But is there a pattern here?" he wondered.

"Well, 11 is the first prime number whose square is greater than 113." Jenny saw a pattern. "We didn't have to check anything greater than $\sqrt{113}$."

PRIME TESTING SHORTCUT

1. Check only prime numbers as possible divisors of your number.
2. Find the first prime number p whose square is greater than the number you are testing. You don't have to check anything greater than p.

   (In other words, you only have to check primes up to the square root of your number.)

"If we want to find whether 343 is a prime number, what is the largest prime we have to test to see whether it divides 343?" Jenny wondered.

Peter started multiplying primes. He skipped the first few because he knew they were too small.

$$11 \times 11 = 121$$
$$13 \times 13 = 169$$
$$17 \times 17 = 289$$
$$19 \times 19 = 361$$

"OK," said Peter, "We see that 19 is the first prime number whose square is greater than 343. By our rule, we only have to test primes less than 19 to see whether they are divisors of 343." (This is Problem 1a.)

Jenny decided to try a larger number. "Is 1019 prime?" she wondered.

"$40 \times 40 = 1600$. That is more than 1019, so I don't have to check for prime divisors greater than 40.

"$30 \times 30 = 900$. That is less than 1019—I have to check primes greater than 30.

"$31 \times 31 = 961$. Still less than 1019. I have to go higher.

"$37 \times 37 = 1369$.

"To test whether 1019 is a prime number, I have to test only the primes less than 37," Jenny concluded. "Since 31 is the last prime before 37, I only have to check through 31."

"I did it another way," said Jesse. "I used the square root key on my calculator. When we look for divisors of 1019, we only have to test prime numbers whose squares are less than 1019. These are the primes that are less than $\sqrt{1019}$. My calculator says $\sqrt{1019} \approx 31.92$. Since $\sqrt{1019}$ is between 31 and 32, we don't have to check any numbers higher than 31.

✎ **Do Problem 1 now.**

PROBLEMS
(Workbook page W115)

1. Find whether the following are prime numbers. Explain how you know.

a. 343 **b.** 1019
c. 1369 **d.** 2417
e. 2573 **f.** 1007

The Sieve of Eratosthenes

One method for finding prime numbers is called the **Sieve of Eratosthenes** (*air-uh-TAHS-thuh-neez*). It is named after a Greek mathematician who lived in North Africa around 230 BC.

"What is a sieve?" asked Evie.

"I know," said Abby. "It is a strainer, like the one my parents use to separate the spaghetti from the water."

The Sieve of Eratosthenes is a way of separating the prime numbers from the composite numbers. It involves crossing out all numbers that are divisible by 2, then all numbers divisible by 3, then numbers divisible by the next number not yet crossed out, and so on. The numbers that survive are the ones that are not divisible by other numbers (except 1), so the numbers that survive are prime.

THE SIEVE OF ERATOSTHENES

A. Cross out 1 since it is not prime.

B. Circle 2 since it is prime. Then cross out all remaining multiples of 2, since they can't be prime. (Why not?)

C. Circle 3, the next prime. Cross out all remaining multiples of 3, since they can't be prime.

D. Circle the next number that hasn't been crossed out. It is prime. (Why?) Cross out all remaining multiples of that number.

E. Repeat Step D until all numbers are either circled or crossed out.

"I'll try the sieve method on the numbers from 1 to 50 to see how it works," said Lilah. "Then I'll try it again and watch more closely for a pattern."

✎ **Do Problems 2–5 now.**

PROBLEMS
(Workbook pages W116–W118)

2. Follow the steps in the Sieve of Eratosthenes to find all prime numbers from 1 to 50.

3. As you followed the steps in Problem 2, you probably found that multiples of the larger prime numbers had already been crossed out. What was the largest prime whose multiples were not already crossed out by smaller numbers?

4. **a.** Use the Sieve of Eratosthenes to find all primes between 1 and 130. Each time you work with a new prime, make a note telling the first of its multiples not already crossed out by a smaller prime. (For example, when the prime is 3, the first multiple to consider is 6 but that has already been crossed out. Therefore, 9 is the first multiple of 3 not already crossed out by a smaller prime.)

b. Look at your notes from **4a**. Describe a pattern that tells, for any prime number, its first multiple not already crossed out by smaller prime numbers.

c. When sieving for primes between 1 and 130, what was the largest prime that had multiples that were not already crossed out by smaller numbers?

d. After you had crossed out the multiples of enough primes, you could stop because only prime numbers were left. When did this happen?

5. **a.** Suppose that you used the sieve method to find the primes between 1 and 200. List the primes whose multiples you would have to cross out before only primes were left. Explain why.

b. Suppose that you used the sieve method to find the primes between 1 and 1000. List the primes whose multiples you would have to cross out before only primes were left.

Counting Primes

Peter used the sieve to find all primes between 1 and 100. But he didn't stop there. He found all primes between 1 and 1000. He made the table at the right.

Peter noticed that the number of primes in an interval seemed to be going down as the numbers increased. He wondered whether this pattern continued. He decided to go to the library to see if he could find out more. He found a book there that gave a list of primes. He counted the primes in the list and added these lines to his table (*below right*).

"There seem to be fewer and fewer primes as the numbers get larger," he observed. "I wonder if you ever run out of primes. Wow. That would mean there is a largest prime number!"

"No," said Lilah. "It doesn't matter how large a prime number you find. There will always be one that is larger. This is how I know:

"Suppose you have a list of all the primes there are. Multiply them all together. You get a really big number, $N = 2 \times 3 \times 5 \times 7 \times \ldots$. That number N is divisible by every prime on your list, right?"

"Of course it is, since it is a multiple of every prime on my list. I'm with you so far," said Peter.

"Good. Now add 1," Lilah continued. "You get $N + 1$, which cannot be divisible by 2."

"Let me think about that," said Peter. "I get multiples of two by counting by 2s, so the first number after N that is divisible by 2 is $N + 2$. So, I agree, $N + 1$ can't be divisible by 2."

Interval	Number of primes in interval
1 to 100	25
101 to 200	21
201 to 300	16
301 to 400	16
401 to 500	17
501 to 600	14
601 to 700	16
701 to 800	14
801 to 900	15
901 to 1000	14

Interval	Number of primes in interval
1 to 1000	168
1001 to 2000	135
9001 to 10,000	72

"OK," said Lilah, "and $N + 1$ also cannot be divisible by 3, since the first number after N that is divisible by 3 is $N + 3$."

"I see." Peter was following this reasoning. "And for a similar reason, $N + 1$ can't be divisible by any of the primes on my list."

"Right—and that means that either $N + 1$ is a prime number or it is divisible by a prime number not on your list. Either way, it must be that there is another prime."

"But how could that be, since you told me I had a list of *all* the prime numbers there are?" Peter was confused.

"It must be you didn't really have a list of *all* the primes. We can always find another prime—we'll never run out of primes."

Peter was disappointed—he had liked the idea that there might be a largest prime number. But Lilah was delighted to have convinced him otherwise.

What Lilah had explained was known to the Greeks more than 2000 years ago. It is called Euclid's Theorem. Here it is:

Euclid's Theorem: There are infinitely many prime numbers.

Formulas for Finding Primes

The Cryptokids wondered whether they could find a formula to generate all the prime numbers, but there is no such formula. They discovered, however, that there are formulas to describe some primes.

Twin primes are primes of the form p and $p + 2$. The numbers 3 and 5 are twin primes, as are 11 and 13. No one knows whether or not there are infinitely many pairs of twin primes.

Mersenne numbers are numbers of the form $2^n - 1$. A monk named Father Marin Mersenne worked with these numbers in the 1600s. The first Mersenne number is $2^1 - 1 = 1$. The second is $2^2 - 1 = 3$. If the exponent n is composite, then the corresponding Mersenne number is

composite. However, if the exponent n is prime, the corresponding Mersenne number can be either prime or composite.

For example, 4 is composite, and $2^4 - 1 = 64 - 1 = 63$, which is also composite ($63 = 3^2 \times 7$). The number 3 is prime, and $2^3 - 1 = 8 - 1 = 7$, which is prime.

Many of the largest known primes are Mersenne primes. In fact, one way people have found very large prime numbers is to test large Mersenne numbers to see whether they are prime.

A **Sophie Germaine prime** is a prime p such that $2p + 1$ is also prime. For example, 2, 3, and 5 are Sophie Germaine primes, but 7 is not, since $2 \times 7 + 1 = 15$, which is not prime. These primes were named after a French mathematician who lived about 200 years ago. No one knows whether or not there are infinitely many Sophie Germaine primes.

"How are these special numbers going to be useful to us?" Peter asked Tim.

"Well, we need large prime numbers for keys in the RSA cipher, or otherwise our ciphers will be too easy to break," Tim replied. "We can check numbers that might be Mersenne primes, Sophie Germaine primes, and twin primes—or other special primes. That's easier than checking all numbers."

"That's a good idea," said Evie. "Since most numbers are not prime, it would waste time to check every number."

✎ **Do Problems 6–10 now.**

PROBLEMS
(Workbook pages W119–W120)

6. **a.** One attempt at a formula to generate prime numbers is $n^2 - n + 41$. Evaluate the formula for $n = 0, 1, 2, 3, 4, 5$. Do you always get a prime?

b. Challenge. Find an n less than 50 for which the formula does not generate a prime.

7. Look back at your list of primes. Find all pairs of twin primes between 1 and 100.

8. Find the Mersenne numbers for $n = 5$, 6, 7, and 11. Which of these are prime?

9. Find at least three Sophie Germaine primes other than 2, 3, and 5.

10. Challenge. Find a large prime number. (You decide whether it is large enough to please you.) Explain how you chose the number and how you know it is prime.

Peter came to the next meeting of the Cryptoclub very excited.

"You know what I read? Regular people have found new prime numbers. In 1978, two high school kids found a new Mersenne prime. At the time, it was the largest known prime number. This news made the front page of the *New York Times*. Now people can join the Great Internet Mersenne Prime Search to hunt for Mersenne primes. In 2005, a volunteer found a Mersenne prime with 7,816,230 digits!"

"That is huge!" said Tim. "The largest number I knew about before was a googol. A **googol** is 10^{100}. You write it as 1 followed by 100 zeros. So a googol has only 101 digits. It's tiny compared to the largest known prime numbers."

"I am surprised people are still discovering new things about math," said Abby. "I thought all math was discovered a long time ago."

Abby didn't realize that mathematics is a changing subject, not one that was completely figured out hundreds of years ago. Some mathematicians work on new problems such as how to find fast methods for computers to factor numbers. Others work on problems that were posed long ago but have not yet been solved. For example, a very famous statement about primes was made by Christian Goldbach (1690–1764). It is called the **Goldbach Conjecture**. It says that every even number greater than 2 is the sum of two primes. For example, 8 = 3 + 5. Even though the Goldbach conjecture is simple to state, no one knows yet whether it is true or false.

✎ **Do Problem 11 now.**

PROBLEMS
(Workbook page W121)

11. **a.** Test the Goldbach Conjecture: Pick several even numbers greater than 2 and write each as the sum of two primes. (Don't use 1 in your sums, since 1 is not prime.)

b. Find a number that can be written as the sum of two primes in more than one way.

DO YOU KNOW?
The Great Internet Mersenne Prime Search

The Great Internet Mersenne Prime Search (GIMPS) is a project of volunteers who work together to find Mersenne primes using special software available for free on the Internet. The search is responsible for the discovery of eight Mersenne primes, each of which was the largest known prime when it was discovered. GIMPS was founded by George Waltmann in 1997.

The exciting thing about the GIMPS project is that anyone can participate in the research. Sometimes entire school classrooms have participated. When you sign up, you receive a program that uses your computer to search for primes. Your computer runs the program while you are doing other things, like sleeping. It will let you and the GIMPS project know if it finds anything.

In February 2005, a new largest-known prime number was found by Dr. Martin Nowak, an eye surgeon in Michelfeld, Germany. It is $2^{25,964,951} - 1$ and has 7,816,230 digits. The previous largest prime was found by Josh Findley about a year before that.

To read more about the GIMPS project you can visit their website, http://www.mersenne.org/.

Finding Primes without Factoring
The Sieve of Eratosthenes

This is a procedure to find all the prime numbers on a list of consecutive numbers.

Cross off 1.

Circle 2 – it is a prime number because its only factors are 1 and 2.
Cross off all multiples of 2.

Circle the next number that is not crossed off -- this number is a prime number because it would have been crossed off if it has a factor smaller than itself.
Cross off all multiples of that number.

Repeat the previous two steps until the number you circle has no multiples on the page that are not already crossed off.

Finally, circle all the rest of the numbers that haven't been crossed off yet. They are all prime numbers because each one cannot be a multiple of any of the smaller numbers.

Notice: For this 200 chart, the first uncircled number that has no multiples left is 17. One way to see this is to notice that 17^2 (= 289) is greater than 200. All smaller multiples (2·17, 3·15, up to 16·17) have already been crossed off because they have factors that are smaller than 17.

1	2	3	4	5	6	7	8	9	10
11	12	13	14	15	16	17	18	19	20
21	22	23	24	25	26	27	28	29	30
31	32	33	34	35	36	37	38	39	40
41	42	43	44	45	46	47	48	49	50
51	52	53	54	55	56	57	58	59	60
61	62	63	64	65	66	67	68	69	70
71	72	73	74	75	76	77	78	79	80
81	82	83	84	85	86	87	88	89	90
91	92	93	94	95	96	97	98	99	100
101	102	103	104	105	106	107	108	109	110
111	112	113	114	115	116	117	118	119	120
121	122	123	124	125	126	127	128	129	130
131	132	133	134	135	136	137	138	139	140
141	142	143	144	145	146	147	148	149	150
151	152	153	154	155	156	157	158	159	160
161	162	163	164	165	166	167	168	169	170
171	172	173	174	175	176	177	178	179	180
181	182	183	184	185	186	187	188	189	190
191	192	193	194	195	196	197	198	199	200

In general, if you have a chart that ends with a number, N, you know to stop as soon as you get to a number whose square it greater than N. In advance you can compute this number by finding $\sqrt{N}$.

1	2	3	4	5	6	7	8	9	10
11	12	13	14	15	16	17	18	19	20
21	22	23	24	25	26	27	28	29	30
31	32	33	34	35	36	37	38	39	40
41	42	43	44	45	46	47	48	49	50
51	52	53	54	55	56	57	58	59	60
61	62	63	64	65	66	67	68	69	70
71	72	73	74	75	76	77	78	79	80
81	82	83	84	85	86	87	88	89	90
91	92	93	94	95	96	97	98	99	100

Primes to 10,000 without Factoring

No calculators are allowed. In this project we are going to all work together to find all of the prime numbers less than 10,000. We will be doing this using a little bit of addition and subtraction, but no division.

Prerequisites. Everyone must understand how the Sieve of Eratosthenes works. You should be able to do it and explain on the grid of 200 numbers. We will be using the same technique on a grid of numbers up to 10,000. To save space no even numbers have been included on the grid we will be using. Each group has a different section of the grid.

Each group has a chart that looks almost like a combination chart. Each row increases by 2 going across and each column increases by 40 going down. They are not combination charts. The numbers do not represent combinations of two numbers. Zero is not on the chart. All of the numbers are odd. But arrow movements are still valid. A right arrow, → moves once to the right and represents +2. A down arrow, ↓ moves down and represents +40.

Your group's X001 chart includes all of the odd numbers from X001 to X999, where X = 1, 2, 3, 4, 5, 6, 7, 8 or 9. We will all be working on the 1001 Chart. We need to pass certain information from group to group about prime numbers as we go.

- We must tell the next group where to find the first multiple of the next prime. When your group is ready to pass information to the next group, one person will set your chart above the next chart and figure out where the cricket will land.

- We share information on cricket movements that advance through multiples of the given prime number.

When you know the largest multiple of a prime number on the previous chart, you can figure out the first multiple of that prime on your chart using a cricket move. Then following that cricket through your chart you can cross off all multiples of that prime. When you find the largest multiple of that prime on your chart you add that multiple to the class table so that the next group can get started.

When crosses off multiples in your group, work on two copies of the grid. Call off the multiples so you know that you agree on each number you cross off and so that you don't miss any numbers that should be crossed off. One mistake early on will trickle down through the entire project.

We need to know when to stop. Because $100^2 = 10{,}000$, we know we have to keep going through all the multiples of all the primes less than 100.

There is an Infinite Number of Prime Numbers

That there is an infinite number of prime numbers seems plausible to most people. Sometimes a student will say that this is so because there are an infinite number of numbers so we must need an infinite number of prime numbers to generate them all. These students wouldn't be able to understand why the proof given here is necessary.

To help this student understand what is going on it might first be useful to try to understand why it might be possible to have a finite number of prime numbers that would be capable of generating an infinite number of integers.

Task: Find all the numbers generated by 2, 3, 5.

2, 3, 4, 5, 6, 8, 9, 10, 12,

1. How do I know that I can get an infinite number?

So I get an infinite number of numbers but not all of them. For example, I'm missing 7 and 11. But maybe I just need to add a few more.

Task: Find all the numbers generated by 2, 3, 5, 7. What's missing?

Task: Find all the numbers generated by all of the prime numbers we found in the Primes to 10,000. How might I find a bigger number that is not generated by all those prime numbers?

Problems:

2. Is the number $2 \cdot 3 \cdot 5 + 1$ a prime number? If not, what is the next smallest prime number that divides it?

3. Is the number $2 \cdot 3 \cdot 5 \cdot 7 + 1$ a prime number? If not, what is the next smallest prime number that divides it?

4. Is the number $2 \cdot 3 \cdot 5 \cdot 7 \cdot 11 + 1$ a prime number? If not, what is the next smallest prime number that divides it?

5. Is the number $2 \cdot 3 \cdot 5 \cdot 7 \cdot 11.13 + 1$ a prime number? If not, what is the next smallest prime number that divides it?

Explain: If I multiply all the prime numbers together, up to a certain point, and add 1, I either get a new prime number or a number that has a prime factor larger than any of the prime numbers in my original product. This is because my number is +1 more than a multiple of each prime and hence not a multiple of that prime.

Unique Factorization

Every number has a unique prime factorization.

Once again this theorem is hard to understand because it seems so true for anyone who has had experience with numbers and factoring. So we want to explore why it might be possible to think that it's not true. The first thing to notice is that it is not true for composite numbers – this sometimes tricks people. For example,

$$24 = 4*6 \text{ and also } 24 = 3*8$$

OF course, these numbers can be further factored into prime numbers and in either case if we keep factoring we end up with $2\cdot2\cdot2\cdot3$. But how do I know that this will always be the case for *any number* I start with

Explanation in here.

TRUE or FALSE $a|b\cdot c$ then $a|b$ or $a|c$
(If a is a factor of $b\cdot c$ then a is a factor of b or a is a factor of c

Examples:

THEOREM: If p is a prime number,
$p|b\cdot c$ then $p|b$ or $p|c$

(If p is a factor of $b\cdot c$ then p is a factor of b or p is a factor of c)

PROOF:

If p is not a factor of b then gcd(b,p) = 1 so by the Extended Euclidean Algorithm:

$$Xp + Yb = 1$$

multiply this equation by c to get

$$Xpc + Ybc = c$$

Now, p is a factor of the first term, Xpc, and p is also a factor of the second term because $p|b\cdot c$ so p is a factor of the LHS so it must also be a factor of the RHS so p is a factor of c.

Teaching Presentation: Exponents

1. Read Sections 6.1 – 6.4 in the CME Algebra I packet. Do enough exercises so you are comfortable with the ideas of each section.

2. Our goal is to be able to explain why

$$b^0 = 1, \text{ for all } b \neq 0 \quad \text{and} \quad b^{-1} = \frac{1}{b}, \text{ for all } b \neq 0$$

3. You will be assigned one of three problems to present:

   Page 514 #14 and #15.
   Page 517 Minds in Action Episode 23
   Page 518 Minds in Action Episode 24

4. Find two problems from earlier in the chapter that you think promote learning about exponents in a way that will make answers easier to understand.

Complete the pink and write the solutions to both problems. You choice. Hand in one copy and keep a copy for yourself. The class period after the proposal is due you will be expected to present the problem to one of the instructors.

assignment	date	grade
Proposal		/20
Group Practice Presentation		/10
Class presentation		/10
Related Problem		/10

Pink Sheet: Maneuvers

Name: Date:

State the problem your group was given to present.

State the two other problems you found to support learning –give page numbers as well.

1.

2.

Investigation Overview

Similar to Chapter 1, this investigation focuses on extending patterns and concepts to generate new mathematical knowledge. Students extend the basic rules of exponents to find sensible definitions for the zero exponent and negative exponents.

You may wish to assign Questions 1–3 for students to think and write about during the investigation.

Learning Goals

- Make calculations involving integral exponents.
- Simplify expressions involving integral exponents.
- Explain and apply the basic rules of exponents.
- Calculate with the zero exponent and negative exponents.
- Explain why the definitions for zero and negative exponents emerge from the basic rules of exponents.

Habits and Skills

- Use numerical examples and counterexamples to think about abstract principles, such as exponential identities.
- Understand the meaning of exponential notation.
- Multiply, add, subtract, and divide with exponents.
- Extend concepts and patterns to build new mathematical knowledge.

Investigation 6A

Exponents

In *Exponents*, you will learn about integral (or integer) exponents. You will use the rules of exponents to make calculations. You will undo exponents to solve equations. You also will calculate using the zero exponent and negative exponents.

By the end of this investigation, you will be able to answer questions like these.

1. What are the basic rules of exponents?
2. Explain why 2^0 is equal to 1.
3. How can you write $\frac{2^3 \cdot 2^{-2} \cdot 2^7}{(2^5)^3 \cdot 2^{-2}}$ as a number without exponents?

You will learn how to

- make calculations involving integral exponents
- simplify expressions involving integral exponents
- explain and apply the basic rules of exponents
- calculate with the zero exponent and negative exponents

You will develop these habits and skills:

- Understand the meaning of exponential notation.
- Multiply, add, subtract, and divide with exponents.
- Extend concepts and patterns to build new mathematical knowledge.

A gecko has about 1×10^6 setae on its feet. Each seta branches into about 1×10^3 spatulae.

Investigation Road Map

LESSON 6.1, *Getting Started,* has students experiment with "proposed basic rules" of exponents. By presenting their examples and counterexamples to the class, students will gain a working knowledge of the basic rules of exponents.

LESSON 6.2, *Squares, Cubes, and Beyond,* reviews the basics of positive integral exponents.

LESSON 6.3, *More Basic Rules of Exponents,* formalizes the basic rules of exponents that the students explored in Lesson 6.1.

LESSON 6.4, *Zero and Negative Exponents,* extends the basic rules of exponents to find sensible definitions for the zero exponent and negative exponents.

LESSON 6.5, *Scientific Notation,* introduces the basics of scientific notation. Scientific examples illustrate the usefulness of the notation.

6.1 Getting Started

Activating Prior Knowledge
Exploring New Ideas

You may think of multiplication as repeated addition. The product $4 \cdot 3$ can mean "add 3 copies of 4 together."

$$4 \cdot 3 = \underbrace{4 + 4 + 4}_{\text{3 copies of 4}}$$

You may know that exponents work in a similar way. The expression 4^3 means "multiply 3 copies of 4 together."

$$4^3 = \underbrace{4 \cdot 4 \cdot 4}_{\text{3 copies of 4}}$$

In general, if n is a positive integer, a^n is the product of n factors of a. You read a^n as "a to the n."

$$a^n = \underbrace{a \cdot a \cdot a \cdot \cdots \cdot a}_{n \text{ copies of } a}$$

You call a the **base** and n the **exponent**.

What does a^1 mean? It may not look like a product, but it means that there is one factor of a.

$$a^1 = \underbrace{a}_{\text{1 copy of } a}$$

Here are some examples of expressions with exponents.

$$a^4 = a \cdot a \cdot a \cdot a$$
$$a^{10} = a \cdot a \cdot a \cdot a \cdot a \cdot a \cdot a \cdot a \cdot a \cdot a$$

Two exponents have special names. To **square** a number means to multiply the number by itself. The expression a^2 ("a squared") means $a \cdot a$. You can square any expression, including expressions with integers, fractions, and variables.

$a^2 = a \cdot a$
$\left(\frac{2}{5}\right)^2 = \frac{2}{5} \cdot \frac{2}{5} = \frac{2^2}{5^2} = \frac{4}{25}$
$(-3)^2 = (-3) \cdot (-3) = 9$
$12^2 = 12 \cdot 12 = 144$
$(4w)^2 = 4w \cdot 4w = 4^2 \cdot w^2 = 16w^2$

Similarly, to **cube** a number means to multiply the number times the number times the number. In other words, you find the product of the number's square and the number. The expression a^3 ("a cubed") means $a \cdot a \cdot a$. You can cube any expression.

$a^3 = a \cdot a \cdot a$
$\left(\frac{1}{5}\right)^2 = \frac{2}{5} \cdot \frac{2}{5} \cdot \frac{2}{5} = \frac{2^3}{5^3} = \frac{8}{125}$
$(-3)^3 = (-3) \cdot (-3) \cdot (-3) = -27$
$12^3 = 12 \cdot 12 \cdot 12 = 1728$
$(4w)^3 = 4w \cdot 4w \cdot 4w = 4^3 \cdot w^3 = 64w^3$

Lesson Overview

GOAL

- Warm up to the ideas of the investigation.

This lesson exposes students to the basic rules of exponents, as well as some "false" basic rules. By experimenting with both the true and false rules, the students will gain an understanding of the differences between rules that "look true," such as $a^b + a^c = a^{b+c}$, and rules that are true, such as $a^b \cdot a^c = a^{b+c}$.

FOR YOU TO EXPLORE
- Core: 1, 2, 3
- Optional: 4

HOMEWORK
- Core: 9
- Optional: 5, 6, 7, 8

VOCABULARY
- case
- cube of a number
- exponent
- square of a number

Launch

Divide students into small groups and assign Problems 1, 2 and 3. Let the students in each group know that they will need to present their findings to the class with examples and/or counterexamples. You may wish to give each group a few transparencies to assist with the presentations.

Explore

For You to Explore

PROBLEM 2 Allow each group to explore the "proposed basic rules" until they reach a group consensus about which are true. You may wish to have each group explore two sets of rules so they can check each other's conclusions. Groups can present their findings to the rest of the class, including the examples they used to draw their conclusions. Encourage students to pay particular attention to the rules that are true.

Note: Examples alone, though perhaps convincing, are not absolute proof that any of these rules are always true. Depending on students's ability and time constraints, you may ask some students to consider how they would prove that a basic rule will always be true.

PROBLEM 4 Encourage students to break up the larger strings into smaller strings and find the number of combinations for each smaller string. For example, break up the 9-digit string into nine 1-digit strings. For each 1-digit string there are 10 choices. So, there is a total of 10^9 choices.

Another method is to break up the 9 digits into the traditional Social Security Number strings of 3 digits-2 digits-4 digits. So, the total number of Social Security Numbers is $(10^3)(10^2)(10^4)$.

Wrap Up

After the groups present their findings to the class, make a list of the proposed rules that the students believe are true.

For You to Explore

1. There are 9 square feet in a square yard. There are 27 cubic feet in a cubic yard. Explain.
2. Here are some additional basic rules, but they are not all true. Substitute numbers for a, b, and c to check whether each equation is true. Decide whether each rule could be a basic rule. Use numerical examples as evidence. Write a convincing argument that summarizes your conclusions.

Group I

$a^b \stackrel{?}{=} (-a)^b$

$a^{b+c} \stackrel{?}{=} a^b + a^c$

$a^{b+c} \stackrel{?}{=} a^b \cdot a^c$

Group II

$a^b \stackrel{?}{=} b^a$

$a^b \cdot a^c \stackrel{?}{=} a^{bc}$

$(a^b)^c \stackrel{?}{=} a^{bc}$

Group III

$(a^b)^c \stackrel{?}{=} a^{(b^c)}$

$(a^b)^c \stackrel{?}{=} a^b \cdot b^c$

$\frac{a^b}{a^c} \stackrel{?}{=} a^{b-c}$

Group IV

$(ab)^c \stackrel{?}{=} a^c \cdot b^c$

$a^b \stackrel{?}{=} a(a^{b-1})$

$(ab)^c \stackrel{?}{=} a(b^c)$

3. Write each expression as a power of 6.

   a. $6^{51}6^{48}$ **b.** $(6^5)^7$ **c.** $6(6^{25}6^{14})$ **d.** $\frac{6^{95}}{6^{19}}$

   You will write each result using a base of 6 and an exponent. For example, 6^{14}.

4. Everyone who is born in the United States is eligible to receive a Social Security number that has nine digits. You can divide the digits into groups of three digits, two digits, and four digits. How many possible Social Security numbers are there?

Express your answer in two different ways.

a. Find how many different nine-digit combinations are possible. Express this result as a power of 10.

b. Think about dividing the nine digits into groups of three digits, two digits, and four digits. How many different combinations are possible for three digits? For two digits? For four digits? Can you use the number of combinations to find the total possible number of Social Security numbers?

Answers

For You to Explore

1. There are 3 ft in a yard. (3 ft)(3 ft) = 9 square feet. (3 ft)(3 ft)(3 ft) = 27 cubic feet.
2. I: Only the third rule is true. II: Only the third rule is true. III: Only the third rule is true. IV: The 1st and 2nd rules are true; check students' explanations.
3. **a.** 6^{99} **b.** 6^{35} **c.** 6^{40} **d.** 6^{76}
4. **a.** 10^9
   b. $10^3 \cdot 10^4 \cdot 10^2$

Exercises Practicing Habits of Mind

On Your Own

5. Some states make license plates using combinations of three letters followed by three numbers. That is, you can have "ABC 123" on a license plate, but not "123 ABC." Using combinations of three letters followed by three numbers, how many license plates are possible?

6. Many garage door openers use a four-digit code, where each digit can be any number from 0 to 9. What is the total number of possible four-digit codes? Explain.

7. If the code for a garage door opener is only two digits long, how many codes are possible? How many three-digit codes are possible? Explain.

In Exercises 6 and 7, express your answer as a power of 10.

8. Most credit card numbers are 16 digits long.

a. If each digit can be any number from 0 to 9, how many different credit numbers are possible? Express your result in different ways. (**Hint:** Divide the 16 digits into smaller groups. Then, use your results from Exercises 6 and 7.)

b. Some credit card numbers have special digits. Suppose a card's number must start with 37 followed by a nonzero digit. Then the 13 following digits can be any number from 0 to 9. How many different credit numbers are possible?

Maintain Your Skills

9. Rewrite each expression using exponents.

a. $x \cdot x \cdot x \cdot 3 \cdot 3 \cdot y \cdot y$

b. $a \cdot b \cdot b \cdot b \cdot 3 \cdot b \cdot a \cdot b \cdot a$

c. $2 \cdot 3 \cdot m \cdot m \cdot m$

d. $x \cdot x \cdot x \cdot x \cdot \frac{1}{x}$

Go Online Video Tutor
PHSchool.com
Web Code: bde-0775

Exercises

5. $26^3 \cdot 10^3 = 17{,}576{,}000$

6. 10^4; there are ten choices for each digit, and four digits.

7. 10^2; 10^3; you have 10 choices for each digit. If there are n digits, the total number of choices is $10 \cdot 10 \cdot 10 \ldots$, a total of n tens.

8. a. 10^{16} **b.** $9 \cdot 10^{13}$

9. a. $9x^3y^2$ **b.** $3a^3b^5$

c. $6m^3$ **d.** x^3

Exercises

HOMEWORK
- Core: 9
- Optional: 5, 6, 7, 8

On Your Own

EXERCISE 5 One method for solving these types of exercises is to first draw a picture of the available slots.

__ __ __ __ __ __

Then fill in the number of choices in each slot. The first three slots are letters, and there are 26 possible letters. So, there are 26 choices for each of these slots.

26 26 26 __ __ __

The last three slots are digits, and there are 10 possible digits. So, there are 10 choices for each of these slots.

26 26 26 10 10 10

Finally, multiply everything together. Students can apply this method to almost all of the exercises in this lesson. It may be worth noting that states do not necessarily assign every possible license plate number.

EXERCISE 7 helps students think about exponents as repeated multiplication.

EXERCISE 8 The different ways of expressing the product may reflect some of the basic rules of exponents that the students verified in For You to Explore. For example, 10^{16} is equivalent to $(10^4)^4$. The equality $10^{16} = (10^4)^4$ is an example of the basic rule $(a^b)^c = a^{bc}$, where $a = 10$, $b = 4$, and $c = 4$.

Lesson Overview

GOALS

- Make calculations involving integral exponents.
- Simplify expressions involving integral exponents.
- Explain and apply the basic rules of exponents.

If your students are struggling, you may consider spending additional time on this lesson. On the other hand, students may have seen some of this material, so this material may be review. With an advanced class, you could consider skimming, or even skipping this lesson. In this lesson, students prove that $a^b a^c = a^{b+c}$. The basic rules of exponents are important throughout mathematics.

CHECK YOUR UNDERSTANDING
- Core: 1, 2, 4, 5
- Optional: 6, 7, 8a–b
- Extension: 3, 8c

HOMEWORK
- Core: 9, 11, 14, 17
- Optional: 10, 12, 13, 15, 16

Launch

Review Problem 3 and Exercise 9 from Lesson 6.1.

Explore

When discussing Theorem 6.1, you may want to explore why the diagram style for $(3^b)(3^c) = 3^{b+c}$ essentially proves the theorem. Because the students have not yet learned about negative or noninteger exponents, Theorem 6.1 is limited to positive integers b and c.

6.2 Squares, Cubes, and Beyond

In Chapter 1, you explored the any-order, any-grouping properties (AOAG) for both addition and multiplication. In Lesson 6.1, you may have noticed that there is no AOAG property for exponents. For instance,

$$2^{20} = 1{,}048{,}576, \text{ but } 20^2 = 400.$$

In general, changing the order of exponents changes the outcome. This example shows that the any-order part of AOAG does not work.

Most of the time, $a^b \neq b^a$. What are some examples where they are equal?

For Discussion

1. Check the any-grouping part of AOAG by comparing $(3^2)^4$ and $3^{(2^4)}$. Are they equal? Use a few other examples, such as $(2^3)^4$ and $2(3^4)$. Does the any-grouping part of AOAG work for exponents?

The convention for a^{b^c} is to consider it as $a^{(b^c)}$.

While there is no AOAG for exponentiation, there are some basic rules for exponents. In Lesson 6.1, you explored a collection of proposed basic rules. Group I explored one of these rules.

$$a^b \cdot a^c = a^{b+c}$$

Why is this rule true? Try it with numbers. For example, $(3^2)(3^5)$.

$$(3^2)(3^5) = \underbrace{(3 \cdot 3)}_{2 \text{ copies}} \cdot \underbrace{(3 \cdot 3 \cdot 3 \cdot 3 \cdot 3)}_{5 \text{ copies}} = \underbrace{(3 \cdot 3 \cdot 3 \cdot 3 \cdot 3 \cdot 3 \cdot 3)}_{2 + 5 = 7 \text{ copies}} = 3^7$$

When you multiply 3^2 and 3^5, there are a total of 7 factors of 3. You use the same process when you find the product $(3^b)(3^c)$.

$$(3^b)(3^c) = \underbrace{(3 \cdot 3 \cdot \ldots \cdot 3)}_{b \text{ copies}} \cdot \underbrace{(3 \cdot 3 \cdot \ldots \cdot 3)}_{c \text{ copies}} = \underbrace{(3 \cdot 3 \cdot \ldots \cdot 3)}_{b + c \text{ copies}} = 3^{b+c}$$

This argument works if the base is 2, -1, $\frac{1}{2}$, or even a variable, such as a. Now that you have an argument, or proof, you can write the theorem. This simple statement, the Law of Exponents, is very important to the discussion of exponents.

Theorem 6.1 ***The Law of Exponents***

For any number a and positive integers b and c, $a^b \cdot a^c = a^{b+c}$.

You can only use Theorem 6.1 if the bases are the same. Consider the following.

$7^3 \cdot 7^8 = 7^{3+8} = 7^{11}$ $\qquad$ $6^3 \cdot 7^8 \neq (6 \cdot 7)^{3+8}$

Answers

For Discussion

1. $(3^2)^4 \neq 3^{(2^4)}$; no

For You to Do

Simplify each expression.

2. example: $a^2 \cdot a^5 = a^7$

3. $k^8 \cdot j^7 \cdot k^{13}$

4. $m^4(m^5)$

5. $r^3(s^7 + r^2)$

6. $4^3 \cdot x^2 \cdot 4 \cdot x^2$

7. $2^3x^3(2x)^2$

For Discussion

8. Use Theorem 6.1 and the basic rules for addition and multiplication to prove that $a^b \cdot a^c \cdot a^d = a^{b+c+d}$.

For You to Do

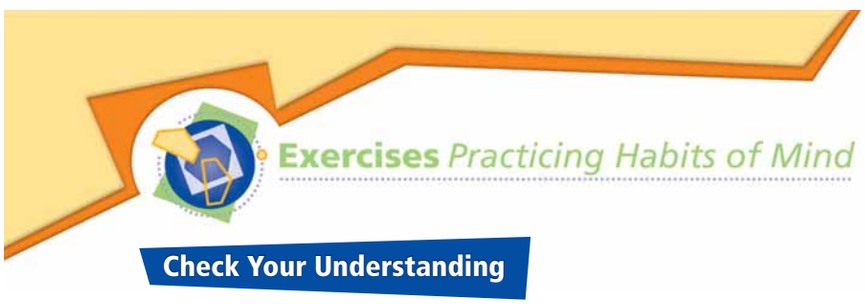
9. **What's Wrong Here?** Matt simplifies the expression $(4m)^3 - 2m - 2m(2m^2 - 1)$ as shown.

$$(4m)^3 - 2m - 2m(2m^2 - 1) = 4m^3 - 2m - 4m^3 + 2m$$
$$= 0$$

Emily simplifies the same expression in another way.

$$(4m)^3 - 2m - 2m(2m^2 - 1) = 64m^3 - 2m - 4m^3 + 2m$$
$$= 60m^3$$

Who is correct? Explain what one of the students did wrong.



Check Your Understanding

1. Without using a calculator, find which of the following expressions is equal to 2^{12}. Explain.

a. $2^{10} + 2^2$ **b.** 2^62^6 **c.** $(2^{10})(2^2)$ **d.** $(2^4)(2^3)$

e. $(2^4)(2^4)(2^4)$ **f.** $2^9 + 2^3$ **g.** $2^{11} + 2^{11}$ **h.** $4(2^{10})$

For You To Do

2. a^7 **3.** j^7k^{21}

4. m^9 **5.** $r^3s^7 + r^5$

6. 4^4x^4 or $(4x)^4$

7. $(2x)^5$ or 2^5x^5

For Discussion

8. By Theorem 6.1, $a^b \cdot a^c \cdot a^d = (a^b \cdot a^c) \cdot a^d = a^{b+c} \cdot a^d$. Use Theorem 6.1 again to get $a^{b+c} \cdot a^d = a^{b+c+d}$.

For You To Do

9. Emily is right; $(4m)^3 = 4^3m^3 = 64m^3$, $(4m)^3 \neq 4m^3$.

Exercises

1. See back of book.

For You to Do

PROBLEM 9 Help students understand why $(4m)^3 = 64m^3$. Explain that since $4m$ is inside the parentheses, you cube both 4 and m. Also, encourage your students to try it with numbers. They can plug in any nonzero number to confirm this identity.

Wrap Up

Discuss some subset of Check your Understanding Exercises 6–8.

Assessment Resources

Lesson Quiz 6.2

1. Identify the expressions equivalent to 3^{16}. Do not use a calculator.

a. $3^4 \cdot 3^4$ **b.** $(3^4)^4$ **c.** $3 \cdot 3^{16}$ **d.** $3^{10} + 3^6$

e. $(3^7)(3^4)(3^5)$ **f.** $9(3^{14})$ **g.** $(3^8)(3^8)$ **h.** $(3^2)^8$

2. Use the rule $(ab)^n = a^nb^n$ to simplify each expression.

a. $2^4 \cdot 5^4$ **b.** $(30^3)\left(\frac{1}{10}\right)^3$ **c.** $20^3 \cdot 5^3$

d. $(8)^{15}\left(\frac{1}{8}\right)^{15}$ **e.** $\left(\frac{2}{3}\right)^4\left(-\frac{3}{2}\right)^4$ **f.** $\left(\frac{14}{2}\right)^2\left(\frac{10}{7}\right)^2$

3. Rewrite each expression using exponents.

a. $x \cdot x \cdot x \cdot y \cdot y \cdot y$ **b.** $a \cdot a^2 \cdot a^4 \cdot 5 \cdot 5 \cdot b \cdot b$

c. $z \cdot z \cdot z^3 \cdot z^2 \cdot 4z$ **d.** $(4x)^4 \cdot x \cdot x^6$

4. Solve for the value of x.

a. $3^x = 27$ **b.** $3^{x-1} = 9$ **c.** $3^{5x} = 81$ **d.** $(3^x)(3^x) = 81$

Exercises

HOMEWORK

- Core: 9, 11, 14, 17
- Optional: 10, 12, 13, 15, 16

Check Your Understanding

EXERCISE 1 reviews the basics of exponential expressions. Students should complete the exercise without a calculator and justify their answers. Remind students that although they could just evaluate 2^{12} and each of the expressions, it is simpler to apply the basic rules.

EXERCISE 2 captures an essential connection between decimal notation and scientific notation, which students will explore in Lesson 6.5. The number 10^n has n digits.

EXERCISE 4 Proofs do not need to be formal for this exercise. Look for an argument such as:

- Multiply n copies of (ab).
- Remove all the parentheses.
- Push all of the a's to the front, and all of the b's to the back.
- You have n copies of a (a^n) and you have n copies of b (b^n), which is $a^n b^n$.

You may want to discuss this exercise with your class.

EXERCISE 5 Students should complete this exercise without a calculator. Each expression is of the form $a^n b^n$, but it is simpler to think of the expression as $(ab)^n$. For example, $5^7 2^7 = (5 \cdot 2)^7 = (10)^7$.

EXERCISE 6 asks students to write exponential expressions from word problems. Part (d) considers a permutation, choosing letters without duplicates.

EXERCISE 7 If the students answer Exercise 6 correctly, then this exercise is simply a matter of remembering how to calculate percentages.

EXERCISE 8 gives students more practice in writing exponential expressions from word problems. Part (c) is a bit tricky, because it matters whether p is even or odd.

2. **Write About It** If you write 10^6, 10^9, and 10^n in standard form, how many zeroes are in each number? Explain.

3. **Take It Further** Suppose you expand $10^2 \cdot 5^3 \cdot 3^5 \cdot 2 \cdot 10^3 \cdot 8$ and write it as a single integer. Starting on the right, how many zeros are there from the units digit to the first nonzero digit?

4. Explain why the rule $(ab)^n = a^n b^n$ is true. It may help to draw diagrams similar to the diagrams at the beginning of this lesson.

In Lesson 6.1, Group IV explored this rule.

5. Use the rule from Exercise 4 to simplify each expression.

a. $5^3 2^3$ **b.** $4^6 25^6$ **c.** $9^{10}\left(\frac{1}{9}\right)^{10}$

d. $20^4\left(\frac{1}{10}\right)^4$ **e.** $20^4 5^4$ **f.** $\left(\frac{4}{3}\right)^4\left(\frac{15}{2}\right)^4$

6. Use the 26 letters in the English alphabet.

a. How many different combinations of three letters are possible? For example, NEK, KEN, and BBR are combinations.

b. How many different combinations of n letters are possible?

c. How many different three-letter combinations use all consonants?

d. How many different three-letter combinations use all different letters?

The vowels are A, E, I, O, and U. Consider the rest of the letters as consonants.

7. In one English dictionary, there are the following numbers of words.

- 2 one-letter words
- 96 two-letter words
- 1238 three-letter words
- 3391 four-letter words

Only 2 out of the 26 possible one-letter sets are words.

a. If you write a letter at random, what is the probability that you form a word? Write your result as a percent. Round to two decimal places.

b. If you write two letters at random, what is the probability that you form a word? Write your result as a percent. Round to two decimal places.

c. Which is more likely, forming a word using three random letters, or forming a word using four random letters?

8. A palindrome is a string of letters that is the same whether you read it backwards or forwards.

a. How many different combinations of three letters are palindromes? An example is EVE.

b. How many different combinations of four letters are palindromes? An example is OTTO.

c. **Take It Further** How many different combinations of p letters are palindromes?

Answers

2. 10^6: 106, 109, and 10n have 6 zeros, 9 zeros, and n zeros respectively; when you multiply a number by 10, it has the effect of adding one zero to the end of the number.

3. 8

4. Answers may vary. Sample: In the product $(ab)(ab)(ab)\ldots$ (where (ab) is multiplied n times), there are n instances of a, and n instances of b. By AOAG, the product equals $(aaa\ldots)(bbb\ldots) = a^n b^n$.

5. **a.** 10^3 **b.** 100^6 **c.** 1
d. 2^4 **e.** 100^4 **f.** 10^4

6. **a.** 26^3 **b.** 26^n **c.** 21^3
d. $26 \cdot 25 \cdot 24 = 15{,}600$

7. **a.** 7.69% **b.** 14.20%
c. The three-letter word is more likely.

8. **a.** 26^2 **b.** 26^2
c. If p is even, there are $26^{\frac{p}{2}}$. If p is odd, there are $26^{\frac{(p+1)}{2}}$.

On Your Own

9. Rewrite each expression using exponents.

a. $x \cdot y \cdot x \cdot y \cdot x \cdot y \cdot x$ **b.** $m \cdot m^2 \cdot m^3 \cdot 3 \cdot 3 \cdot n \cdot n$

c. $z \cdot z \cdot z^4 \cdot 5z$ **d.** $(2x)^3 \cdot x \cdot x^3$

10. A National Football League field is $53\frac{1}{3}$ yards wide and 120 yards long including both end zones. How many square feet are in a football field?

11. **a.** If $2^x = 8$, what is the value of x?

b. If $2^{y-1} = 16$, what is the value of y?

c. If $2^{5z} = 64$, what is the value of z?

d. If $(2^w)(2^w) = 64$, what is the value of w?

12. A craftsperson designs Russian nesting dolls so that each doll fits inside of the next larger doll. In a set of nesting dolls, the smallest doll, Doll 0, is 1 inch tall.

Note that these dolls are not drawn to scale.

Suppose each doll is twice as tall as the previous doll. How tall is each of the following dolls?

a. Doll 1 **b.** Doll 3

c. Doll 8 **d.** Doll n

Go Online PHSchool.com

For additional practice, go to **Web Code:** bda-0602

On Your Own

EXERCISE 10 allows students to practice unit conversions.

ERROR PREVENTION In Exercise 10, some students may multiply $53\frac{1}{3}$ by 120 and then multiply by 3. This results in an incorrect answer. Students should multiply by 9 if they calculate this way. It may be worthwhile to explore why this answer is incorrect.

EXERCISE 11 reviews powers of 2 and the basics of exponents and expressions. Since students do not know logarithms, there is no systematic way to solve exercises of this type. Students need to remember facts about powers of 2, such as $2^6 = 64$, and work backwards from there.

EXERCISE 12 Students will see these nesting dolls again in Lesson 6.3 as a preview of zero and negative exponents.

9. **a.** x^4y^3 **b.** $9m^6n^2$

c. $5z^7$ **d.** $8x^7$

10. 57,600 square feet

11. **a.** 3 **b.** 5 **c.** $\frac{6}{5}$ **d.** 3

12. **a.** 2 in. **b.** 8 in.

c. 256 in. **d.** 2^n in.

EXERCISE 13 is a good exercise to demonstrate to students that $0.75 \cdot 2^n$ is different from $(0.75 \cdot 2)^n$.

Additional Resources

PRINTED RESOURCES
- Texas Instruments Activities Workbook
- Cabrilog Activities
- Teaching Resources
- Practice Workbook
- Assessment Resources

TECHNOLOGY
- TeacherExpress CD-ROM
- **Exam***View* CD-ROM
- **PHSchool.com**
  - Homework Help
  - Video Tutors
  - Multiple Choice
  - Crosswords

Additional Practice

1. Rewrite each expression using exponents.
a. $x \cdot x \cdot y \cdot x \cdot x \cdot y$ **b.** $a \cdot 3 \cdot b^2 \cdot a^2 \cdot 3 \cdot b$ **c.** $m \cdot m^6 \cdot m \cdot 3m$
d. $(2a)^2 \cdot (2a)^2 \cdot (2a) \cdot a^3$ **e.** $(3x)^2 \cdot (2x)^3$ **f.** $2 \cdot 3 \cdot 4 \cdot x \cdot x^2 \cdot x^3$

2. What is the value of s in each equation?
a. $3^s = 81$ **b.** $3^{s-2} = 81$ **c.** $3^{2s} = 81$
d. $3^s \cdot 3^s = 729$ **e.** $4^{s-1} = 64$ **f.** $5^s \cdot 5^s \cdot 5^s = 125$

3. Suppose a photocopier makes copies at 125% of the original size. A picture is 4 inches wide. If each copy serves as the original for the next copy, how wide is the picture on each copy?
a. the first copy **b.** the second copy
c. the sixth copy **d.** the nth copy

4. Suppose a photocopier makes copies at 80% of the original size. Each copy serves as the original for the next copy. If the picture is 6 inches wide, how wide is the picture on each copy?
a. the first copy **b.** the second copy
c. the sixth copy **d.** the nth copy

5. Which of the following are identities?
a. $\left(-\frac{1}{x}\right)^1 = -\left(\frac{1}{x}\right)^1$ **b.** $\left(-\frac{1}{x}\right)^2 = -\left(\frac{1}{x}\right)^2$ **c.** $\left(-\frac{1}{x}\right)^3 = -\left(\frac{1}{x}\right)^3$
d. $\left(-\frac{1}{x}\right)^4 = -\left(\frac{1}{x}\right)^4$ **e.** $\left(-\frac{1}{x}\right)^5 = -\left(\frac{1}{x}\right)^5$ **f.** What is the pattern?

6. Decide whether each expression equals 7^8, without using a calculator. Explain each result.
a. $7 \cdot 7 \cdot 7 \cdot 7 \cdot 7 \cdot 7 \cdot 7 \cdot 7$ **b.** $7^4 \cdot 7^2$ **c.** $\frac{7^{16}}{7^2}$ **d.** $\frac{7^4 \cdot 7^3 \cdot 7^3}{7^2}$

7. Write each expression as a single power of m.
a. $(m^3)^5$ **b.** $(m^5)^3$ **c.** $(m^9)^9$ **d.** $\frac{m^{15}}{m^{12}}$ **e.** $\frac{1}{m^4}(m^9)$

8. For each sequence, find a pattern. Use your pattern to write the next three terms in each sequence.
a. 729, 243, 81 **b.** 10,000; 1000; 100 **c.** $8^3, 8^2, 8^1$
d. $\frac{1}{625}, \frac{1}{125}, \frac{1}{25}$ **e.** $\left(\frac{1}{3}\right)^3, \left(\frac{1}{3}\right)^2, \left(\frac{1}{3}\right)^1$ **f.** $5^5, 5^4, 5^3$

Practice: For Lesson 6.2, assign Exercises 1–5.

13. In a different set of Russian dolls, Doll 0 is only 0.75 inch tall. Suppose each doll is twice as tall as the previous doll. How tall is each of the following dolls?
a. Doll 1 **b.** Doll 3
c. Doll 8 **d.** Doll n

14. **Standardized Test Prep** What is the value of the expression $2 \cdot 2^2 \cdot 2^3$?
A. 20 **B.** 32
C. 64 **D.** 128

Maintain Your Skills

15. Simplify each expression.
a. 1
b. $1 + 10$
c. $1 + 10 + 10^2$
d. $1 + 10 + 10^2 + 10^3$
e. $1 + 10 + 10^2 + 10^3 + 10^4$
f. $1 + 10 + 10^2 + 10^3 + 10^4 + 10^5$
g. What is the pattern of the sums?

16. Simplify each expression.
a. $4 \cdot 1$
b. $4 \cdot 1 + 9 \cdot 10$
c. $4 \cdot 1 + 9 \cdot 10 + 5 \cdot 10^2$
d. $4 \cdot 1 + 9 \cdot 10 + 5 \cdot 10^2 + 2 \cdot 10^3$
e. $4 \cdot 1 + 9 \cdot 10 + 5 \cdot 10^2 + 2 \cdot 10^3 + 4 \cdot 10^4$
f. $4 \cdot 1 + 9 \cdot 10 + 5 \cdot 10^2 + 2 \cdot 10^3 + 4 \cdot 10^4 + 7 \cdot 10^5$
g. $4 \cdot 1 + 9 \cdot 10 + 5 \cdot 10^2 + 2 \cdot 10^3 + 4 \cdot 10^4 + 7 \cdot 10^5 + 2 \cdot 10^6$
h. What is the pattern of the sums?

Go Online Video Tutor
PHSchool.com
Web Code: bde-0775

Answers

13. **a.** 1.5 in. **b.** 6 in.
c. 192 in. **d.** $0.75 \cdot 2^n$ in.

14. C

15. **a.** 1 **b.** 11 **c.** 111
d. 1111 **e.** 11,111 **f.** 111,111
g. Each number is made up of all 1's.

16. **a.** 4 **b.** 94 **c.** 594
d. 2594 **e.** 42,594 **f.** 742,594
g. 2,742,594
h. Each power of 10 determines the place value of each digit.

17. Which of the following are identities?

a. $(-x)^1 \stackrel{?}{=} -x^1$

b. $(-x)^2 \stackrel{?}{=} -x^2$

c. $(-x)^3 \stackrel{?}{=} -x^3$

d. $(-x)^4 \stackrel{?}{=} -x^4$

e. $(-x)^5 \stackrel{?}{=} -x^5$

f. What is the pattern in the exponents?

This sand sculpture contains an estimated 10^{11} grains of sand.

Historical Perspective

A *googol* is a famous large number equal to 10^{100}. The mathematician Edward Kasner used this large number in a book he was writing in 1940. He asked his 9-year-old nephew, Milton Sirotta, for a name for the number. Milton replied, "Googol." The name stuck.

How large is a googol? Here is what it looks like.

10,000,000,000,000,000,000,000,000,000,000,000,000,000,000,000,000, 000,000,000,000,000,000,000,000,000,000,000,000,000,000,000,000, 000,000,000

A googol is much larger than the number of grains of sand on Earth or the number of known stars in the sky. In fact, some astronomers estimate that there are between 10^{72} and 10^{87} particles in the entire known universe. That is much smaller than a googol.

A googolplex is another number that is even larger than a googol. A googolplex looks like this.

$$10^{(10^{100})} \text{ or } 10^{\text{googol}}$$

You can write a googolplex with a 1 followed by a googol zeros. This number is so large that you cannot even write all the zeros. If you tried to write all the zeros of a googolplex in a book, the book would be larger than the entire universe!

Go Online PHSchool.com

For more information about a googol, go to **Web Code:** bde-8031

17. (a), (c), and (e) are identities; odd powers of $-x$ are negative.

Historical Perspective

The story exhibits a playful side of some mathematicians, both in the choice of the word *googol* and in the decision to name such an inconceivably large number. For example, if a googol is greater than the number of particles in the entire universe, why would you ever need to talk about a googolplex? You may not, but since you assume that the numbers "go on forever," there is nothing to stop you from naming or thinking about such a number.

Lesson Overview

GOALS

- Make calculations involving integral exponents.
- Simplify expressions involving integral exponents.
- Explain and apply the basic rules of exponents.

This lesson introduces division of exponential expressions and raising exponential expressions to powers. You should emphasize numerical examples and the intuition underlying Theorems 6.2 and 6.3. These theorems may be review for some students.

CHECK YOUR UNDERSTANDING

- Core: 1, 2, 3, 4
- Optional: 5, 6, 7

HOMEWORK

- Core: 9, 10, 12, 16
- Optional: 8, 11, 13, 14, 15

Launch

Have your students read the introductory text at the beginning of the lesson.

Explore

For You to Do

PROBLEM 4 provides a good opportunity to help your students understand the meaning of Theorem 6.2.

6.3 More Basic Rules of Exponents

There is a rule for dividing powers that have the same base.

For You to Do

1. Express $\frac{3^5}{3^3}$ as a power of 3.
2. Express $(2^4)^3$ as a power of 2.
3. Express $(xy)^4$ without using parentheses.

To divide two exponential expressions with the same base, such as 2^7 and 2^3, you can rewrite the exponents as repeated multiplication.

$$\frac{2^7}{2^3} = \frac{\overbrace{2 \cdot 2 \cdot 2 \cdot 2 \cdot 2 \cdot 2 \cdot 2}^{7 \text{ copies}}}{\underbrace{2 \cdot 2 \cdot 2}_{3 \text{ copies}}} = \frac{2 \cdot 2 \cdot 2 \cdot \overbrace{2 \cdot 2 \cdot 2 \cdot 2}^{7 - 3 \text{ copies}}}{2 \cdot 2 \cdot 2} = 2^{7-3} = 2^4$$

You can cancel three copies of 2 in the numerator and three copies in the denominator. You are left with $7 - 3$, or 4, copies of 2 in the numerator.

For You to Do

4. Make a diagram like the one above to simplify $\frac{3^5}{3^3}$.

Theorem 6.2

For any number $a \neq 0$ and positive integers b and c where $b > c$, $\frac{a^b}{a^c} = a^{b-c}$.

In this investigation, you will find a way to remove the restriction $b > c$.

For Discussion

5. Prove Theorem 6.2 by making a diagram like the one above to show that $\frac{a^b}{a^c} = a^{b-c}$. Assume that $b > c$ and $a \neq 0$.
6. How does your diagram change if $b < c$?

Answers

For You To Do

1. 3^2 2. 2^{12} 3. x^4y^4

For You To Do

4. See back of book.

For Discussion

5. See back of book.
6. Answers may vary. Sample: There will be more copies of the letter left in the denominator.

For You to Do

Compute each quotient, without a calculator.

7. $\frac{10^9}{10^8}$ **8.** $\frac{6^3x^9}{3^32^2x^5}$ **9.** $\frac{2^2}{2^5}$

To raise an exponent to another exponent, you can rewrite the exponents as repeated multiplication. For example, how many copies of 7 are in $(7^5)^3$?

$$(7^5)^3 = \underbrace{\underbrace{(7 \cdot 7 \cdot 7 \cdot 7 \cdot 7)}_{5 \text{ copies}} \cdot \underbrace{(7 \cdot 7 \cdot 7 \cdot 7 \cdot 7)}_{5 \text{ copies}} \cdot \underbrace{(7 \cdot 7 \cdot 7 \cdot 7 \cdot 7)}_{5 \text{ copies}}}_{3 \text{ copies of } 7^5} = 7^{5 \cdot 3} = 7^{15}$$

Each 7^5 includes five copies of 7. There are three copies of each 7^5, which gives a total of $5 \cdot 3$, or 15, copies of 7.

$$(7^5)^3 = 7^{5 \cdot 3} = 7^{15}$$

For You to Do

10. Make a diagram like the one above to simplify $(2^4)^3$.

These results lead to the third basic rule of exponents.

Theorem 6.3

For any number *a* and positive integers *b* and *c*, $(a^b)^c = a^{bc}$.

For You to Do

Expand each expression.

11. $(2^2)^3$ **12.** $(x^6)^7$

To write an expression, such as $(xy)^4$, without parentheses, multiply the expression by itself.

$$(xy)^4 = \underbrace{xy \cdot xy \cdot xy \cdot xy}_{4 \text{ copies}}$$

Remember that xy means $x \cdot y$. You can use AOAG to rearrange the factors. You can place all the x's together first, and then place all the y's together.

$$(xy)^4 = x \cdot y \cdot x \cdot y \cdot x \cdot y \cdot x \cdot y = \underbrace{x \cdot x \cdot x \cdot x}_{4 \text{ copies}} \cdot \underbrace{y \cdot y \cdot y \cdot y}_{4 \text{ copies}} = x^4y^4$$

THEOREM 6.3 You may want to explore with your students why they can generalize from both the diagram and the discussion for $(3^5)^4$ to prove this theorem.

For You to Do

7. 10 **8.** $2x^4$ **9.** $\frac{1}{8}$

For You To Do

10. See back of book.

For You To Do

11. 2^6 **12.** x^{42}

PROBLEM 13 provides a good opportunity to help your students understand the meaning of Theorem 6.4.

Wrap Up

For Discussion Problem 6 is a good preparation for Lesson 6.4. Discuss this problem with your students to encourage them to think about the concept of negative exponents.

Assessment Resources

Lesson Quiz 6.3

1. Identify the expressions equivalent to 4^{12}. Do not use a calculator.
   a. $(4^{10})^2$ b. $(4^3)^4$ c. $(4^7)(4^5)$ d. $4^5 + 4^5$
   e. $(4^6)(4^2)$ f. $(4^4)^3$ g. $(4^{12})(4)$ h. $16(4^{10})$
   i. $(4^3)\,(4^3)\,(4^3)\,(4^3)$ j. $2^2 \cdot 4^{11}$ k. $4^{10} + 4^2$ l. $(4^{24})^{\frac{1}{2}}$
2. Identify the expressions equivalent to 5^3. Do not use a calculator.
   a. $\frac{a^8}{a^5}$ b. $\frac{5^{27}}{5^{24}}$ c. $\frac{5^{15}}{5^5}$ d. $(5^2)^1$
   e. $\frac{(5^2)^3}{5^3}$ f. $\frac{5^{10} \cdot 5^3}{5^{10}}$ g. $5 + 5 + 5$ h. $5^2 + 5$
   i. $(5^2)(5)$ j. $\frac{(5^3)^8}{(5^7)^3}$ k. $\frac{1}{5} \cdot 5^4$ l. $(5^{\frac{1}{3}})(5^9)$
3. **Multiple Choice** If $A = x^4$ and $B = x^3$, which expression is a way to write x^{11} in terms of A and B?
   A. AB B. A^2B C. AB^2 D. $A + A + B$

Exercises

HOMEWORK
- Core: 9, 10, 12, 16
- Optional: 8, 11, 13, 14, 15

Check Your Understanding

EXERCISE 1 Ask your students, "How can you get a sum of 8 by adding just 2's and/or 3's?" Students may find this question easier than the exercise, but it is essentially the same question.

EXERCISE 2 focuses on approximating large calculations, an important, yet often overlooked, skill.

For You to Do

13. Make a diagram like the one above to simplify $(7a^2b)^3$.

Theorem 6.4

For any numbers *a* and *b*, and positive integer *m*, $(ab)^m = a^m b^m$.

Corollary 6.4.1

For any numbers *a* and *b* ($b \neq 0$) and positive integer *m*, $\left(\frac{a}{b}\right)^m = \frac{a^m}{b^m}$.

For Discussion

14. Prove Theorem 6.4 by making a diagram like the one above to show that $(ab)^m = a^m b^m$.

15. Prove Corollary 6.4.1 without making a diagram. (*Hint:* Use Theorem 6.4.)

For You to Do

Expand each expression.

16. $(10x^2)^3$ **17.** $(a^3b)^{11}$ **18.** $\left(\frac{4}{7}\right)^3$ **19.** $\left(\frac{3x^3y^2}{wz^4}\right)^3$

Check Your Understanding

1. Suppose $A = c^3$ and $B = c^2$. Find two ways to write c^8 in terms of A and B.

2. Liz knows that 2^{10} is close to 1000. She estimates the value of 2^{21}. What do you suppose her estimate is?

Answers

For You To Do

13. See back of book.

For Discussion

14. See back of book.

15. Let $c = \frac{1}{b}$.
Then $\left(\frac{a}{b}\right)^m = \left(a \cdot \frac{1}{b}\right)^m = (ac)^m = a^m c^m = a^m \cdot \left(\frac{1}{b}\right)^m = a^m \cdot \left(\frac{1}{b^m}\right) = \left(\frac{a^m}{b^m}\right)$.

For You To Do

16. $1000x^6$ **17.** $a^{33}b^{11}$

18. $\frac{64}{343}$ **19.** $\frac{27x^9y^6}{w^3z^{12}}$

Exercises

1–2. See back of book.

3. Decide whether each expression equals 3^{15}, without using a calculator. Explain each result.

a. $(3^6)^9$ b. $(3^{10})(3^5)$
c. $(3^3)(3^5)$ d. $(3^{15})(3^1)$
e. $(3^5)(3^5)(3^5)$ f. $3^9 + 3^6$
g. $(3^5)^3$ h. $3^{14} + 3^{14} + 3^{14}$
i. $(3^3)^5$ j. $9(3^{13})$
k. $(3^5)^{10}$ l. $(3^1)^{15}$

4. Decide whether each expression equals 2^3, without using a calculator. Explain each result.

a. $\frac{2^6}{2^2}$ b. $\frac{2^6}{2^3}$ c. $(2^2)^1$ d. $\frac{(2^2)^5}{2^7}$
e. $\frac{2^9}{2^6}$ f. $\frac{2^9}{2^3}$ g. $\frac{2^7 2^8}{2^5}$

5. Use the fact that $2^8 = 256$. Find the units digit of 2^{16} and 2^{24}.

6. Find the units digit of $(19^3)^4$.

7. Find the units digit of $(2^5)^2 + (5^2)^2$.

On Your Own

8. In Lesson 6.2, you used a set of Russian nesting dolls. Recall the rule that each doll is twice as tall as the doll before it. For example, Doll 1 is 2 inches tall, and Doll 2 is 4 inches tall. Now, consider two smaller dolls, Doll -1 and Doll -2.

a. How tall is Doll -1? How tall is Doll -2?

b. How tall is Doll -5?

9. **Standardized Test Prep** Simplify the expression $\frac{(2x^2y^3)^3}{4x^4y}$.

A. $\frac{1}{2}x^6y^6$ B. $2xy^5$ C. $\frac{1}{2}x^2y^8$ D. $2x^2y^8$

10. Decide whether each expression equals 5^6, without using a calculator. Explain each result.

a. $5 \cdot 5 \cdot 5 \cdot 5 \cdot 5 \cdot 5$ b. $5^4 5^2$
c. $(5^3)(3^5)$ d. $\frac{5^{15}}{5^9}$
e. $\frac{(5^2)(5^2)(5^3)}{5}$ f. $5^5 + 5$

Go Online PHSchool.com
For additional practice, go to Web Code: bda-0603

EXERCISE 5 exhibits a mathematical application of Theorem 6.3.

On Your Own

EXERCISE 8 previews negative exponents. It may help students gain an intuitive understanding of why the standard definition for negative exponents makes sense.

3. See back of book.
4. See back of book.
5. 6; 6 6. 1 7. 9
8. a. $\frac{1}{2}$ in.; $\frac{1}{4}$ in. b. $\frac{1}{32}$ in.
9. D
10. a. Yes; this is the definition of 5^6, five multiplied by itself six times.
b. yes; $5^4 5^2 = 5^{4+2} = 5^6$
c. No; $(5^3)(3^5)$ is divisible by 3 whereas 5^6 is not.
d. yes; $\frac{5^{15}}{5^9} = 5^{15-9} = 5^6$
e. yes; $\frac{(5^2)(5^2)(5^3)}{5} = \frac{5^7}{5} = 5^{7-1} = 5^6$
f. No; $5^5 + 5 = 5(5^4 + 1)$, which is even, whereas 5^6 is odd.

EXERCISE 12 Part (g) may challenge some students. It may be helpful to show the students that $\frac{1}{b} \cdot a = \frac{a}{b}$.

Additional Resources

PRINTED RESOURCES
- Texas Instruments Activities Workbook
- Cabrilog Activities
- Teaching Resources
- Practice Workbook
- Assessment Resources

TECHNOLOGY
- TeacherExpress CD-ROM
- **Exam***View* CD-ROM
- **PHSchool.com**
  - Homework Help
  - Video Tutors
  - Multiple Choice
  - Crosswords

Additional Practice

1. Rewrite each expression using exponents.
a. $x \cdot x \cdot y \cdot x \cdot x \cdot y$ **b.** $a \cdot 3 \cdot b^2 \cdot a^2 \cdot 3 \cdot b$ **c.** $m \cdot m^6 \cdot m \cdot 3m$
d. $(2a)^2 \cdot (2a)^2 \cdot (2a) \cdot a^3$ **e.** $(3x)^2 \cdot (2x)^3$ **f.** $2 \cdot 3 \cdot 4 \cdot x \cdot x^2 \cdot x^3$

2. What is the value of s in each equation?
a. $3^s = 81$ **b.** $3^{s-2} = 81$ **c.** $3^{2s} = 81$
d. $3^s \cdot 3^s = 729$ **e.** $4^{s-1} = 64$ **f.** $5^s \cdot 5^s \cdot 5^s = 125$

3. Suppose a photocopier makes copies at 125% of the original size. A picture is 4 inches wide. If each copy serves as the original for the next copy, how wide is the picture on each copy?
a. the first copy **b.** the second copy
c. the sixth copy **d.** the nth copy

4. Suppose a photocopier makes copies at 80% of the original size. Each copy serves as the original for the next copy. If the picture is 6 inches wide, how wide is the picture on each copy?
a. the first copy **b.** the second copy
c. the sixth copy **d.** the nth copy

5. Which of the following are identities?
a. $\left(-\frac{1}{x}\right)^1 = -\left(\frac{1}{x}\right)^1$ **b.** $\left(-\frac{1}{x}\right)^2 = -\left(\frac{1}{x}\right)^2$ **c.** $\left(-\frac{1}{x}\right)^3 = -\left(\frac{1}{x}\right)^3$
d. $\left(-\frac{1}{x}\right)^4 = -\left(\frac{1}{x}\right)^4$ **e.** $\left(-\frac{1}{x}\right)^5 = -\left(\frac{1}{x}\right)^5$ **f.** What is the pattern?

6. Decide whether each expression equals 7^8, without using a calculator. Explain each result.
a. $7 \cdot 7 \cdot 7 \cdot 7 \cdot 7 \cdot 7 \cdot 7 \cdot 7$ **b.** $7^4 \cdot 7^2$ **c.** $\frac{7^{16}}{7^2}$ **d.** $\frac{7^4 \cdot 7^3 \cdot 7^3}{7^2}$

7. Write each expression as a single power of m.
a. $(m^3)^5$ **b.** $(m^5)^3$ **c.** $(m^9)^9$ **d.** $\frac{m^{15}}{m^{12}}$ **e.** $\frac{1}{m^1}(m^9)$

8. For each sequence, find a pattern. Use your pattern to write the next three terms in each sequence.
a. 729, 243, 81 **b.** 10,000; 1000; 100 **c.** $8^3, 8^2, 8^1$
d. $\frac{1}{625}, \frac{1}{125}, \frac{1}{25}$ **e.** $\left(\frac{1}{3}\right)^3, \left(\frac{1}{3}\right)^2, \left(\frac{1}{3}\right)^1$ **f.** $5^5, 5^4, 5^3$

Practice: For Lesson 6.3, assign Exercises 6–8.

g. $\frac{5^{18}}{5^{12}}$ **h.** $(5^2)^3$
i. $(5^6)^1$ **j.** $(5^3)^3$
k. $\frac{(5^3)^3}{5^3}$ **l.** $5 + 5 + 5 + 5 + 5 + 5$

11. Use the fact that $4^6 = 4096$. Find the units digit of 4^7 and 4^{12}.

12. Write each expression as a single power of x.
a. $(x^2)^6$ **b.** $(x^2)^5$ **c.** $(x^3)^9$ **d.** $(x^{10})^{10}$
e. $\frac{x^8}{x^2}$ **f.** $\frac{x^9}{x^7}$ **g.** $\frac{1}{x^6}(x^{14})$

13. Simplify each expression.
a. $(7c)^2$ **b.** $(3x^2)^3$ **c.** $\left(\frac{2a}{3bc}\right)^4$
d. $\left(\frac{m^2n^3}{p^4q}\right)^{11}$ **e.** $\left(\frac{2v^3w^2}{8v^2w}\right)^3$ **f.** $4a^2\left(\frac{a^3}{2a^4}\right)^2$

A simplified expression has no parentheses and shows each base only once.

14. ZIP Codes in the United States are five-digit combinations of numbers, such as 48104 or 02134. How many possible five-digit ZIP Codes are there?

15. The United States Postal Service uses the ZIP + 4 Code that adds four extra digits at the end of a ZIP Code. If you live in ZIP Code 48104, your ZIP + 4 Code might be 48104-1126. How many possible nine-digit ZIP + 4 Codes are there? Can you find the result in two ways?

Maintain Your Skills

16. For each sequence, find a pattern. Use your pattern to write the next three terms in each sequence.
a. 256, 128, 64, 32, 16 **b.** 625, 125, 25
c. 27, 9, 3 **d.** $\frac{1}{8}, \frac{1}{4}, \frac{1}{2}$
e. $7^4, 7^3, 7^2$ **f.** $3^3, 3^2, 3^1$
g. $\left(\frac{1}{2}\right)^3, \left(\frac{1}{2}\right)^2, \left(\frac{1}{2}\right)^1$

Answers

g. yes; $\frac{5^{18}}{5^{12}} = 5^{18-12} = 5^6$
h. yes; $(5^2)^3 = 5^{2 \cdot 3} = 5^6$
i. yes; $(5^6)^1 = 5^{6 \cdot 1} = 5^6$
j. no; $(5^3)^3 = 5^{3 \cdot 3} = 5^9$
k. yes; $\frac{(5^3)^3}{5^3} = \frac{5^9}{5^3} = 5^{9-3} = 5^6$
l. No; $5 + 5 + 5 + 5 + 5 + 5 = 6 \cdot 5 = 30$

11. 4; 6
12. **a.** x^{12} **b.** x^{10} **c.** x^{27} **d.** x^{100} **e.** x^6 **f.** x^2 **g.** x^8
13. **a.** $49c^2$ **b.** $27c^6$ **c.** $\frac{16a^4}{81b^4c^4}$ **d.** $\frac{m^{22}n^{33}}{p^{44}q^{11}}$ **e.** $\frac{v^3w^3}{64}$ **f.** 1
14. 10^5
15. 10^9
16. See back of book.

6.4 Zero and Negative Exponents

In Lessons 6.2 and 6.3, you learned the following three basic rules of exponents. For all numbers a and positive integers b and c,

Rule 1 $a^b \cdot a^c = a^{b+c}$

Rule 2 $\frac{a^b}{a^c} = a^{b-c}$, if $a \neq 0$ and $b > c$

Rule 3 $(a^b)^c = a^{bc}$

In each rule, there are annoying restrictions, such as b and c must always be positive integers. Also, for Rule 2, b must be greater than c.

The restrictions exist for the rules because there is no obvious way to describe how to calculate a zero or negative exponent. What does it mean to multiply a number by itself 0 times? What does it mean to multiply a number by itself -4 times?

Recall that in Chapter 1, you defined the meaning of a negative number by expanding an addition table. In episode 23 below, Tony and Sasha explore the definition of a zero exponent. Their goal in developing the definition is to preserve the rules of exponents.

Minds in Action

episode 23

Sasha and Tony are trying to find the value of 2^0.

Sasha $2^0 = 0$ makes sense to me. If 2^5 is five copies of 2, then 2^0 should be zero copies of 2, which is 0.

Tony Yes, that makes some sense. Let's see whether it works with the first basic rule.

$$(a^b)(a^c) = a^{b+c}$$

Sasha Alright. Using our example, we know that $(2^0)(2^5) = 2^{0+5}$.

Tony We can use our definition that $2^0 = 0$ to calculate the value of the left side of the equation.

$$(2^0)(2^5) = (0)(32) = 0$$

Sasha Finding the value of the right side is easy. $0 + 5 = 5$, so $2^{0+5} = 2^5 = 32$. Oh, no.

Tony What?

Sasha Well, now we have found that $0 = 32$, and that's obviously not right. I think we made a bad choice for our definition.

Tony Hmm. We need another definition.

Lesson Overview

GOALS

- Simplify expressions involving integral exponents.
- Explain and apply the basic rules of exponents.
- Calculate with zero exponents and negative exponents.
- Explain why the definitions for zero and negative exponents emerge from the basic rules of exponents.

This lesson extends the basic rules of exponents to derive sensible definitions for the zero exponent and negative exponents.

CHECK YOUR UNDERSTANDING

- Core: 1, 2, 3, 6
- Optional: 4
- Extension: 5

MATERIALS

- Blackline Masters 6.4A and 6.4B

HOMEWORK

- Core: 7, 9, 10, 11
- Optional: 8, 12, 13

VOCABULARY

- negative exponent
- ratio table
- zero exponent

Launch

Jump right into the lesson and review of the basic rules of exponents.

Explore

Minds in Action

The point of this episode is to show students that mathematical definitions are not arbitrary. Students should realize how new mathematical knowledge results from extending old mathematical knowledge. Sasha and Tony extend the basic rules of exponents in order to find a coherent definition of 2^0. If the definition of 2^0 is to continue obeying the basic rules, then 2^0 must equal 1. That is the only choice that will match with the basic rules.

Sasha We want Theorem 6.1 to hold true, right? So, we want $(2^0)(2^5) = 2^{0+5}$.

2^{0+5} is just 2^5. So, we want $(2^0)(2^5) = (2^5)$.

Tony We have no choice. Divide each side of this equation by 2^5, and you have $2^0 = \frac{2^5}{2^5} = 1$.

Sasha So, 2^0 has to be 1. Otherwise, the rules we already know won't keep working.

Remember...

Theorem 6.1 says that if b and c are positive integers, then $a^b \cdot a^c = a^{b+c}$.

For Discussion

1. In the dialogue, Sasha and Tony use the basic rule of multiplying exponents to find a definition of 2^0. Another way to find a definition of 2^0 is to use the basic rule for dividing exponents.

$$\frac{a^b}{a^c} = a^{b-c}$$

If you substitute $a = 2$, $b = 7$, and $c = 7$, you get the following equation.

$$\frac{2^7}{2^7} = 2^{7-7}$$

Explain why this approach produces the same definition that Sasha and Tony found, $2^0 = 1$.

Minds in Action

episode 24

Tony and Sasha discuss possible definitions for 2^{-3}.

Tony Let's try to think this through instead of just guessing what 2^{-3} should be.

Sasha Alright. Well, we want our favorite rule to keep working.

$$(2^b)(2^c) = 2^{b+c}$$

Tony Well, what happens if we say $b = -3$ and $c = 3$?

Sasha I see where you're going. That's genius! Now we can say that $(2^{-3})(2^3) = 2^{-3+3} = 2^0$ since $-3 + 3 = 0$.

Tony Also, $2^0 = 1$, so we have $(2^{-3})(2^3) = 1$.

Sasha We can do what we did for 2^0. Solve for 2^{-3} as if it were an unknown.

$$(2^{-3})(2^3) = 1$$

$$2^{-3} = \frac{1}{2^3}$$

So, $(2^{-3}) = \frac{1}{2^3}$.

For Discussion

PROBLEM 1 The point here is for students to realize that the definition of 2^0 is based on the basic rules. It may not be intuitively obvious to students that 2^0 must equal 1. However, after they see the logic behind the definition, they should be more comfortable with the definition.

Minds in Action

Again, the idea here is to show that the definitions for negative exponents result from the basic rules. The episode focuses on a single example to illustrate the general case. If the definition of 2^{-3} is to continue obeying the basic rules, then 2^{-3} must equal $\frac{1}{2^3}$.

Answers

For Discussion

1. Answers may vary. Sample: The equation $\frac{2^7}{2^7} = 2^{7-7}$ simplifies to $1 = 2^0$.

Tony That surprises me.

Sasha I guess, but if 2^{-3} is going to satisfy the basic rules, that's the only definition that works.

Tony That means $2^{-5} = \frac{1}{2^5}$, $2^{-6} = \frac{1}{2^6}$, and so on.

Sasha So, a negative exponent is like dividing. If you have 2^{-3}, then you divide 1 by 3 factors of 2.

Tony That makes sense. Exponentiation is just repeated multiplication and the opposite of multiplication is division.

For You to Do

2. How can you write $\frac{1}{2^{-3}}$ using only positive exponents?

You can formalize Tony and Sasha's work using these two definitions.

Definition

Zero exponent: If $a \neq 0$, then $a^0 = 1$.

Definition

Negative exponent: If $a \neq 0$, then $a^{-m} = \frac{1}{a^m}$.

Do you understand why these statements are definitions rather than theorems? Are they the only possible definitions of zero and negative exponents?

For Discussion

3. Is the definition of negative exponents compatible with the definition of zero exponents? In other words, do the definitions satisfy the following equations?

- $2^0 = 2^{5+(-5)} = 2^5 \cdot 2^{-5}$
- $a^0 = a^{5+(-5)} = a^5 \cdot a^{-5}$
- $a^0 = a^{b+(-b)} = a^b \cdot a^{-b}$

For You to Do

Apply the basic rules to find the value of each variable. Check your results.

4. $2^5 \cdot 2^{-3} = 2^a$

5. $2^5 \cdot 2^{-7} = 2^b$

6. $\frac{2^5}{2^7} = 2^c$

7. $\frac{2^5}{2^{-7}} = 2^d$

8. $\frac{2^5}{2^c} = 2^8$

For You to Do

PROBLEM 2 Negative exponents and fractions can be daunting for some students, but being able to see the connections between the two is vital for later work with polynomials and rational functions. There are two ways to think about this problem.

- Since $2^{-3} = \frac{1}{2^3}$, then $\frac{1}{2^{-3}} = \frac{1}{\frac{1}{2^3}} = 1 \cdot \frac{2^3}{1} = 2^3$
- You can simplify a fraction of the form $\frac{1}{\frac{a}{b}}$ by taking the reciprocal of the fraction in the denominator. So, $\frac{1}{\frac{1}{2^3}} = \frac{2^3}{1} = 2^3$.

Wrap Up

Restate Theorem 6.2 without the restriction $b > c$ and review For You to Do Problems 4–8.

Assessment Resources

Lesson Quiz 6.4

1. Fill out the table using the given function. Determine whether the table has a constant ratio.

x	$\frac{1}{4}x$	÷
−3		
−2		
−1		
0		
1		
2		
3		

2. Identify the expressions equivalent to 6^{-10}. Do not use a calculator.

a. $\left(\frac{1}{6}\right)^{10}$ b. $\frac{6^3}{6^2 \cdot 6^4 \cdot 6^8}$ c. $(6^5)^{-15}$

d. $6^{-8} \cdot 6^{-2}$ e. $\frac{1}{6^{-10}}$ f. $(6^5)^{-2}$

g. $\frac{1}{(6^5)^2}$ h. $(6^{-5})(6^{-2})$ i. $\frac{6^4}{6^{14}}$

j. $\left(\frac{1}{6^5}\right)^2$ k. $6^{-1} + 6^{-9}$ l. $\frac{6^5}{6 \cdot 6^{-2} \cdot 6^{16}}$

3. Write each expression as a single power of x.

a. $(x^{-3})(x^7)$ b. $\frac{(x^5)^6}{x^2}$ c. $((x^4)^{-4})^{-2}$

d. $\frac{x^{-3} \cdot x^7}{x^3}$ e. $\frac{(x^6)^0}{x^0 \cdot x^{11}}$ f. $\frac{(x^3)^{-2} \cdot x^6}{x^7}$

For You To Do

2. 2^3

For Discussion

3. yes

For You To Do

4. 2

5. −2

6. −2

7. 12

8. −3

Exercises

HOMEWORK
- Core: 7, 9, 10, 11
- Optional: 8, 12, 13

Check Your Understanding

EXERCISES 1 AND 2 You can give students a copy of Blackline Master 6.4A to complete the tables.

EXERCISE 3 highlights the connection between negative exponents and reciprocals.

EXERCISE 4 helps students gain familiarity with exponents by presenting a challenge that is not just a simple calculation. You could mention to your students how this exercise relates to binary (base 2). In binary, each digit corresponds to a power of two. Since you can write any number as the sum of powers of two, without repetition among the powers, then you can write any number in binary as a string of 0's and 1's. For example, since $13 = 2^3 + 2^2 + 2^0$, you can write 13 in binary as 1101. The 0 corresponds to the fact that you do not use 2^1 in the sum.

Exercises *Practicing Habits of Mind*

Check Your Understanding

A ratio table is similar to a difference table from Investigation 5B, except for the last column. A difference table has a Δ column that shows the difference between two consecutive rows. A ratio table has a $\div$ column that shows the ratio between two consecutive rows.

For example, consider this ratio table. The 2 in the first row is the result of dividing the 2 in the second row by the 1 above it. Likewise, the 5 in the third row is the result of dividing 30 by 6. This table does not have constant ratios, since the numbers in the $\div$ column are not all the same.

x	$f(x)$	$\div$
0	1	2
1	2	3
2	6	5
3	30	

For Exercises 1 and 2, copy and complete each table using the given function. Determine whether each table has a constant ratio.

1. $f(x) = 3^x$

x	3^x	$\div$
-3		
-2		
-1		
0		
1		
2		
3		

2. $g(x) = \left(\frac{1}{3}\right)^x$

x	$\left(\frac{1}{3}\right)^x$	$\div$
-3		
-2		
-1		
0		
1		
2		
3		

3. How are the tables in Exercises 1 and 2 related? Explain.

4. Dana says, "You can write any whole number as the sum of powers of 2 without ever repeating any of them."

Andrew replies, "Maybe. What about 13?"

Dana answers, "Let's see. 13 is $2^3 + 2^2 + 2^0$."

Andrew asks, "What about 17?"

Dana explains, "17 is $2^4 + 2^0$."

Is Dana correct? Write each number as a sum of the powers of 2.

a. 14 **b.** 15 **c.** 16 **d.** 31 **e.** 33

Answers

Exercises

1. See back of book.

2. See back of book.

3. The tables are reversed.

4. a. $2^3 + 2^2 + 2^1$

b. $2^3 + 2^2 + 2^1 + 2^0$

c. 2^4

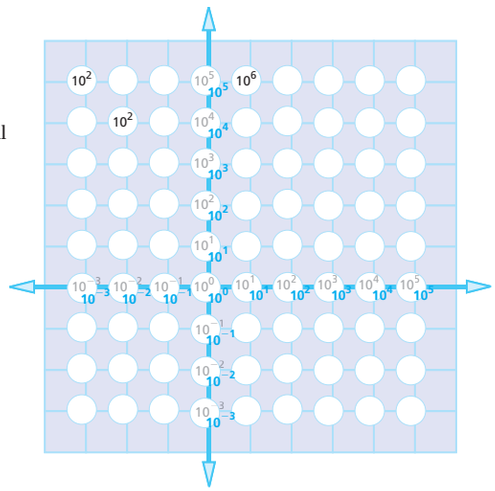
d. $2^4 + 2^3 + 2^2 + 2^1 + 2^0$

e. $2^5 + 2^0$

5. **Take It Further** Prove that Dana is correct for any positive integer n.

6. Copy and complete the table. The multiplication table shows powers of ten, including 10^0, 10^1, 10^2, and so on along the axes. Each square in the table is the product of a number on the horizontal arrow and a number on the vertical arrow. For instance, the upper left corner contains 10^2, since $10^{-3} \cdot 10^5 = 10^{(-3)+5} = 10^2$.

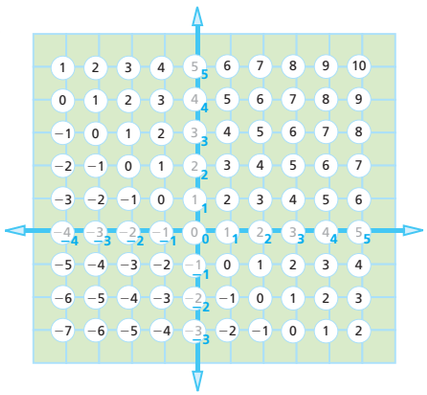
Multiplication Table



On Your Own

7. **Write About It** Compare your results in Exercise 6 to the following part of an addition table. How are the tables similar? Explain.

Addition Table



EXERCISE 6 You can give students a copy of Blackline Master 6.4B so that they do not have to redraw the multiplication table.

On Your Own

EXERCISE 7 If you evaluate $\log_{10}$ for each power of 10 in the multiplication table in Exercise 6, you get the values in the addition table. Students will not see the connection using this language, but they should be able to talk about the similarity of the two tables because $10^a \cdot 10^b = 10^{a+b}$.

5. Answers may vary. Sample: If n is a power of 2, you are done. Suppose n is not a power of 2. Then $2^a < n < 2^{a+1}$ for some integer a. Therefore $n = 2^a + k$ for some integer k less than 2^a. If k is a power of 2, you are done. If not, then $2^b < k < 2^{b+1}$ for some integer $b < a$. Therefore $k = 2^b + m$ for some integer m less than 2^b. Continue with this process. Eventually it will end, because you started with a finite positive integer.

6. See back of book.

7. Answers may vary. The exponents in the multiplication table will match exactly with the entries in the addition table.

EXERCISE 8 reminds students that any number raised to the zero exponent is 1.

Additional Resources

PRINTED RESOURCES
- Texas Instruments Activities Workbook
- Cabrilog Activities
- Teaching Resources
- Practice Workbook
- Assessment Resources

TECHNOLOGY
- TeacherExpress CD-ROM
- **Exam***View* CD-ROM
- **PHSchool.com**
  - Homework Help
  - Video Tutors
  - Multiple Choice
  - Crosswords

Additional Practice

1. Simplify each expression. Assume that $x \neq 0$ and $y \neq 0$.
a. $(2x + 15y)^0$ **b.** $5 \cdot (4x^2y - 2xy^2)^0$ **c.** $x^0 + y^0 + (x + y)^0$

2. Decide whether each expression equals 4^{-8}, without using a calculator. Explain each result.
a. $(4^{-4}) \cdot 4^2$ **b.** $4^{-6} \cdot 4^{-2}$ **c.** $(4^{-5})^{-3}$
d. $(4^2)^{-4}$ **e.** $\frac{4^5}{4^{13}}$ **f.** $\left(\frac{1}{4}\right)^8$
g. $\frac{1}{4^{-8}}$ **h.** $\left(\frac{1}{4^4}\right)^{-2}$

3. Write each expression as a single power of p.
a. $(p^{-6})(p^{11})$ **b.** $((p^2)^3)^{-5}$
c. $\frac{(p^0)^4}{p^8}$ **d.** $\frac{(p^5)^0}{(p^9)(p^{-2})}$

4. Find each sum.
a. 3^0 **b.** $3^0 + 3^1$
c. $3^0 + 3^1 + 3^2$ **d.** $3^0 + 3^1 + 3^2 + 3^3$
e. $3^0 + 3^1 + 3^2 + 3^3 + 3^4$ **f.** What is the pattern of the results?

5. Write each number in scientific notation.
a. 1,000,000 **b.** 47,500 **c.** 512,000,000
d. 202,000 **e.** 0.00231 **f.** 0.00003579
g. $(4.1 \times 10^5)(4 \times 10^7)$ **h.** $(12 \times 10^3)(9 \times 10^4)$ **i.** 153,000 + 2,017,000

6. Write each number in decimal notation.
a. 2.53×10^5 **b.** 4.1032×10^{11} **c.** 1.59×10^{-5}
d. 4.72×10^{-8} **e.** 7.2×10^0 **f.** 5.06×10^{12}

7. Find the mean and median of each set of numbers.
a. $1.2 \times 10^3, 3.4 \times 10^4, 1.6 \times 10^2, 9.8 \times 10^3, 7.5 \times 10^4$
b. $3.21 \times 10^4, 14.5 \times 10^2, 28.2 \times 10^3, 115 \times 10^0, 228 \times 10^3$

8. Express each product or quotient in scientific notation.
a. $(5 \times 10^7)^3$ **b.** $(4 \times 10^9)^2$ **c.** $(6.2 \times 10^5)^2$
d. $\frac{6 \times 10^{12}}{3 \times 10^5}$ **e.** $\frac{9.3 \times 10^{11}}{3 \times 10^5}$ **f.** $\frac{5.2 \times 10^{10}}{4 \times 10^2}$

Practice: For Lesson 6.4, assign Exercises 1–4.

8. Simplify the expression $(4x + 5y - 6z)^0 + (3xy^2 - 5z)^0$. Assume that $4x + 5y - 6z \neq 0$ and $3xy^2 - 5z \neq 0$.

Go Online PHSchool.com
For additional practice, go to **Web Code:** bda-0604

9. Decide whether each expression equals 7^{-10}. Do not use a calculator. Explain each result.
a. $\left(\frac{1}{7}\right)^{10}$ **b.** $7^{-4} \cdot 7^{-3}$ **c.** $(7^{13})(7^{-6})$
d. $\frac{7^3}{7^{13}}$ **e.** $\frac{7^2}{7^3 7^4 7^4}$ **f.** $\frac{1}{7^{-10}}$
g. $7^5 \cdot 7^{-2}$ **h.** $\left(\frac{1}{7^2}\right)^5$ **i.** $(7^5)^{-15}$
j. $(7^5)^{-2}$ **k.** $(7^{-2})^5$ **l.** $\frac{1}{7^{10}}$

10. Write each expression as a single power of z.
a. $(z^{-2})(z^4)$ **b.** $((z^3)^3)^{-3}$ **c.** $\frac{(z^2)(z^{-4})}{z^2}$
d. $\frac{(z^0)^4}{z^{10}}$ **e.** $\frac{(z^7)^0}{(z^0)(z^{11})}$

11. **Standardized Test Prep** Simplify the expression $\frac{a^5b^{-3}}{(a^2b)^0} \cdot \frac{b^2}{a^{-4}}$ where $a \neq 0$ and $b \neq 0$.
A. ab^{-1} **B.** $a^{-1}b^{-2}$ **C.** a^9b^{-1} **D.** a^3b

Maintain Your Skills

12. Find each sum.
a. 2^0 **b.** $2^0 + 2^1$ **c.** $2^0 + 2^1 + 2^2$
d. $2^0 + 2^1 + 2^2 + 2^3$
e. $2^0 + 2^1 + 2^2 + 2^3 + 2^4$
f. $2^0 + 2^1 + 2^2 + 2^3 + 2^4 + 2^5$
g. $2^0 + 2^1 + 2^2 + 2^3 + 2^4 + 2^5 + 2^6$
h. What is the pattern of the results?

13. Find each sum. Express the result as a mixed number, such as $1\frac{2}{3}$.
a. 2^0 **b.** $2^0 + 2^{-1}$ **c.** $2^0 + 2^{-1} + 2^{-2}$
d. $2^0 + 2^{-1} + 2^{-2} + 2^{-3}$
e. $2^0 + 2^{-1} + 2^{-2} + 2^{-3} + 2^{-4}$
f. $2^0 + 2^{-1} + 2^{-2} + 2^{-3} + 2^{-4} + 2^{-5}$
g. $2^0 + 2^{-1} + 2^{-2} + 2^{-3} + 2^{-4} + 2^{-5} + 2^{-6}$
h. What is the pattern of the results?

Answers

8. 2

9. See back of book.

10. **a.** z^2 **b.** z^{-27} **c.** z^{-4} **d.** z^{-10} **e.** z^{-11}

11. A

12. **a.** 1 **b.** 3 **c.** 7 **d.** 15 **e.** 31 **f.** 63 **g.** 127
h. If n is the greatest exponent in the sum, each result is $2^{n+1} - 1$.

13. **a.** 1 **b.** $1\frac{1}{2}$ **c.** $1\frac{3}{4}$ **d.** $1\frac{7}{8}$ **e.** $1\frac{15}{16}$ **f.** $1\frac{31}{32}$ **g.** $1\frac{63}{64}$
h. If n is the least exponent in the sum, each result is $2 - 2^{-n}$.

6.5 Scientific Notation

Using larger numbers can be difficult and confusing. For example, try comparing the masses of the sun and of Earth.

For Discussion

The mass of the sun is about 1,989,000,000,000,000,000,000,000,000,000 kilograms. The mass of Earth is about 5,973,700,000,000,000,000,000,000 kilograms.

1. Does the sun or Earth have the greater mass?
2. What methods did you use to compare the numbers to find the larger number?

To make this comparison much easier, you can use scientific notation to represent any real number uniquely.

Facts and Notation

A number written in scientific notation has the following form.

$$a \times 10^b, \text{ or } -a \times 10^b,$$

where $1 \leq a < 10$ and b is an integer.

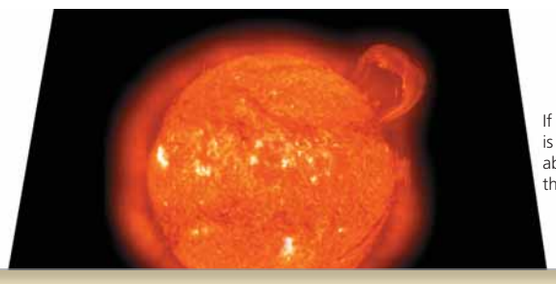
In algebra, you use $\cdot$ more often than $\times$ to represent multiplication. For example, $a \cdot b = a \times b$. Scientific notation is the exception. You write $a \times 10^3$, not $a \cdot 10^3$.

The numbers, 3.7×10^3 and -2.3×10^1, are written in scientific notation. The numbers -3700, 23, and 15×10^3 are not written in scientific notation.

For You to Do

3. Why is 15×10^3 not written in scientific notation?

The restrictions on a may seem arbitrary, but they ensure that there is only one way to write any number in scientific notation.



If the sun's circumference is about 2.7×10^6 mi, about how high did this solar flare reach?

For Discussion

1. the sun
2. Answers may vary. Sample: Count the number of digits.

For You to Do

3. because $15 > 10$

Lesson Overview

GOALS

- Make calculations involving integral exponents.
- Simplify expressions involving integral exponents.
- Explain and apply the basic rules of exponents.
- Calculate with zero exponents and negative exponents.

This lesson introduces the basics of scientific notation. Several examples from science allow students to understand the usefulness of the notation.

CHECK YOUR UNDERSTANDING
- Core: 1
- Optional: 2, 3, 4, 5

HOMEWORK
- Core: 6, 7, 14, 16
- Optional: 8, 9, 10, 11, 12, 13, 15, 17

VOCABULARY
- scientific notation

Launch

Start with For Discussion.

Explore

For Discussion

PROBLEMS 1 AND 2 You may want to have your students compare the number of zeros in each number, and then compare the numbers that remain. For example, the mass of the sun begins with 1989 and ends with 27 zeros, and the mass of Earth starts with 59,737 and ends with 20 zeros. Students probably notice easily that although $59{,}737 > 1989$, the mass of the sun has 7 more zeros, so it is a greater number.

Wrap Up

Review Exercise 1. You may want to work through part (g) together as a class before having students try part (h) on their own.

Assessment Resources

Lesson Quiz 6.5

1. Write each number in scientific notation.

a. 2,745,000 **b.** 832×10^6 **c.** 0.00000931
d. 857,000,000,000,000 **e.** -5 **f.** $(2.7 \times 10^4)(3 \times 10^8)$
g. 0.7×10^7 **h.** $(3.3 \times 10^2)(6 \times 10^3)$ **i.** $-84{,}600{,}000{,}000$
j. $843{,}700 + 2{,}700$ **k.** 0.00074 **l.** 500^3

2. Write each number in decimal notation.

a. 3.47×10^4 **b.** -7.27×10^{-8} **c.** 8.563×10^7
d. 2.2×10^0 **e.** 3.91×10^{-5} **f.** -4.98×10^{13}

3. Express each quotient in scientific notation.

a. $\frac{(10 \times 10^{13})}{(5 \times 10^4)}$ **b.** $\frac{(3.2 \times 10^{23})}{(4 \times 10^{20})}$
c. $\frac{(27 \times 10^6)}{(3 \times 10^2)}$ **d.** $\frac{(8.1 \times 10^{17})}{(9 \times 10^{18})}$

Exercises

HOMEWORK

- Core: 6, 7, 14, 16
- Optional: 8, 9, 10, 11, 12, 13, 15, 17

Check Your Understanding

EXERCISE 2 provides an interesting example of a situation involving division of exponential expressions. Students should not use a calculator. They should be able to explain why the calculation is accurate.

Example

Problem Write 47,000 and 0.0037 in scientific notation.

Solution To write a number in scienitific notation, you "pull out" multiples of 10 until you are left with a number between 1 and 10.

$$\begin{aligned} 47{,}000 &= 4700 \times 10 \\ &= 470 \times 10 \times 10 \\ &= 47 \times 10 \times 10 \times 10 \\ &= 4.7 \times 10 \times 10 \times 10 \times 10 \\ &= 4.7 \times 10^4 \end{aligned}$$

For numbers less than 1, you have to "put in" multiples of 10.

$$\begin{aligned} 0.0037 &= 0.037 \times \frac{1}{10} \\ &= 0.37 \times \frac{1}{10} \times \frac{1}{10} \\ &= 3.7 \times \frac{1}{10} \times \frac{1}{10} \times \frac{1}{10} \\ &= 3.7 \times \left(\frac{1}{10}\right)^3 \\ &= 3.7 \times 10^{-3} \end{aligned}$$

Exercises *Practicing Habits of Mind*

Check Your Understanding

1. Write each number in scientific notation.

a. 1,340,000 **b.** 0.00000609
c. -3 **d.** 0.9×10^5
e. 379×10^5 **f.** 602,000,000,000,000,000,000,000
g. $(1.3 \times 10^5)(6 \times 10^7)$ **h.** $(2.2 \times 10^2)(5 \times 10^4)$

2. Suppose there are approximately 6×10^9 usable telephone numbers in North America that are not assigned. If the government licenses 1×10^8 new telephone numbers each year, how many years will it take until North America runs out of telephone numbers?

Answers

Exercises

1. a. 1.34×10^6 **b.** 6.09×10^{-6}
c. -3×10^0 **d.** 9×10^4
e. 3.79×10^7 **f.** 6.02×10^7
g. 7.8×10^{12} **h.** 1.1×10^7

2. 60 years

3. Use the data from the beginning of this lesson.
   a. Write the masses of Earth and of the sun in scientific notation. Round each decimal to two decimal places. For example, write 1.23×10^9.
   b. How many times more massive is the sun than Earth?
4. Javan measures the length of his hair at the beginning and end of the month. He finds that his hair grows 1 inch per 30 days. How fast does his hair grow in miles per hour? Express your result in scientific notation.
5. Avogadro's number, 6.02×10^{23}, is an important number in chemistry. It represents the number of atoms (or molecules) in one mole of a substance. One mole of carbon weighs 12 grams. How many atoms of carbon do you have if you have 180 grams of carbon? Write your result in scientific notation.

On Your Own

6. Write each number in scientific notation.
   a. 10,000
   b. 93,000
   c. 42,000,000
   d. −86,500,000,000
   e. 0.073
   f. 0.0000119
   g. $(3.5 \times 10^3)(2 \times 10^6)$
   h. $(13 \times 10^2)(5 \times 10^8)$
   i. $13{,}100 + 2600$
   j. 400^3
7. Write each number in decimal notation.
   a. 1.86×10^6
   b. 9.472×10^{10}
   c. 8.46×10^{-4}
   d. -3.77×10^{-10}
   e. 5.5×10^0
   f. -4.09×10^{13}
8. Find the mean and median of the following numbers: 5×10^4, 5×10^3, 5×10^2, 5×10^1, 5. Which is easier to find, the mean or the median?
9. Write each number in scientific notation.
   a. 900×10^6
   b. 7300
   c. 0.8×10^9
   d. 50
   e. 110×10^2
   f. Find the median of the five numbers.

Go Online PHSchool.com
For additional practice, go to Web Code: bda-0605

EXERCISE 3 Show the cancellation of the powers of 10. Note that you can split up the two parts of the fractional computation, since $\frac{a}{b} \times \frac{c}{d} = \frac{ac}{bd}$.

EXERCISE 4 reviews scientific notation and uses negative exponents.

On Your Own

EXERCISE 8 illustrates some of the usefulness of scientific notation. It is easy to see the magnitude of numbers. Thus, it is easier to find the median.

3. a. 1.99×10^{30}; 5.97×10^{24}
   b. about 330,000
4. 2.192×10^{-8} mi/h
5. 9.03×10^{24}
6. a. 1×10^4
   b. 9.3×10^4
   c. 4.2×10^7
   d. -8.65×10^{10}
   e. 7.3×10^{-2}
   f. 1.19×10^{-5}
   g. 7×10^9
   h. 6.5×10^{11}
   i. 1.57×10^4
   j. 6.4×10^7
7. a. 1,860,000
   b. 94,720,000,000
   c. 0.000846
   d. −0.000000000377
   e. 5.5
   f. −40,900,000,000,000
8. The mean is 11,111; the median is 5×10^2; the median.
9. See back of book.

EXERCISES 10–12 ask students to combine their new knowledge of scientific notation with the basic rules of exponents. If students can do Exercises 10–12, then they have learned the essential points of Lessons 6.2 and 6.3. Although these exercises involve large numbers, the numbers are "clean," so students should be able to complete these exercises without using a calculator.

EXERCISE 13 tests students on scientific notation and negative exponents.

10. **Standardized Test Prep** Simplify the expression $\frac{(4.5 \times 10^9)(7.0 \times 10^{-3})}{1.25 \times 10^2}$.

A. 25,200 **B.** 36,000

C. 252,000 **D.** 31,500,000

In Exercises 11–13, you will find which quantity is larger:

- the number of stars in the universe
- the number of grains of sand on the Earth

Which quantity do you think is larger?

The Hubble Telescope sends about 120 gigabytes (giga $= 10^9$) of science data weekly.

11. Based on recent photographs from the Hubble Telescope, scientists estimate that there are 100 billion galaxies. The average galaxy contains 100 billion stars. About how many stars are in the universe? Write your result in scientific notation.

12. Use the following information to estimate the number of grains of sand on Earth.

- 8000 grains of sand are in 1 cubic centimeter of sand.
- 1 million cubic centimeters are in 1 cubic meter.
- 25 billion cubic meters of sand are on Earth.

About how many grains of sand are on Earth? Write your result in scientific notation.

There are 100 centimeters in a meter. Why are there 1,000,000 cubic centimeters in a cubic meter?

13. Based on your estimates, which is greater, the number of stars in the universe or the number of grains of sand on Earth? By what factor is it greater?

14. The planets are constantly in motion, so the distance between Earth and other astronomical objects is constantly changing. The table shows the average distance between Earth and a few astronomical objects.

Average Distance From Earth

Object	Distance (miles)
Moon	2.3×10^4
Mars	1.41×10^8
Neptune	2.7×10^9

SOURCE: United States National Aeronautics and Space Administration

A garden snail moves at the rate of about 3×10^{-2} miles per hour. If a garden snail could fly through space at that rate, how many hours would it take to reach the moon? To reach Mars? To reach Neptune?

Answers

10. C

11. 5.2×10^{22}

12. 2×10^{20}

13. stars; 280

14. 7.67×10^5 h; 4.7×10^9 h; 9.0×10^{10} h

Maintain Your Skills

15. Express each product in scientific notation.

a. $(2 \times 10^5)^3$

b. $(4 \times 10^7)^2$

c. $(3 \times 10^2)^3$

d. $(2.5 \times 10^4)^2$

e. **Take It Further** How can you express the product $(a \times 10^b)^c$ in scientific notation?

16. Express each quotient in scientific notation.

a. $\dfrac{(9 \times 10^{10})}{(3 \times 10^2)}$

b. $\dfrac{(8 \times 10^8)}{(2 \times 10^2)}$

c. $\dfrac{(6.4 \times 10^{12})}{(4 \times 10^7)}$

d. $\dfrac{(3.2 \times 10^{15})}{(8 \times 10^5)}$

17. Simplify each expression.

a. 4×10^0

b. $4 \times 10^0 + 9 \times 10^{-1}$

c. $4 \times 10^0 + 9 \times 10^{-1} + 5 \times 10^{-2}$

d. $4 \times 10^0 + 9 \times 10^{-1} + 5 \times 10^{-2} + 2 \times 10^{-3}$

e. $4 \times 10^0 + 9 \times 10^{-1} + 5 \times 10^{-2} + 2 \times 10^{-3} + 4 \times 10^{-4}$

f. $4 \times 10^0 + 9 \times 10^{-1} + 5 \times 10^{-2} + 2 \times 10^{-3} + 4 \times 10^{-4} + 7 \times 10^{-5}$

g. $4 \times 10^0 + 9 \times 10^{-1} + 5 \times 10^{-2} + 2 \times 10^{-3} + 4 \times 10^{-4} + 7 \times 10^{-5} + 2 \times 10^{-6}$

h. What is the pattern?

Go Online Video Tutor
PHSchool.com
Web Code: bde-0775

Additional Resources

PRINTED RESOURCES
- Texas Instruments Activities Workbook
- Cabrilog Activities
- Teaching Resources
- Practice Workbook
- Assessment Resources

TECHNOLOGY
- TeacherExpress CD-ROM
- **Exam***View* CD-ROM
- **PHSchool.com**
  - Homework Help
  - Video Tutors
  - Multiple Choice
  - Crosswords

Additional Practice

1. Simplify each expression. Assume that $x \neq 0$ and $y \neq 0$.
a. $(2x + 15y)^0$ **b.** $5 \cdot (4x^2y - 2xy^2)^0$ **c.** $x^0 + y^0 + (x + y)^0$

2. Decide whether each expression equals 4^{-8}, without using a calculator. Explain each result.
a. $(4^{-4}) \cdot 4^2$ **b.** $4^{-6} \cdot 4^{-2}$ **c.** $(4^{-5})^{-3}$
d. $(4^2)^{-4}$ **e.** $\frac{4^5}{4^{13}}$ **f.** $\left(\frac{1}{4}\right)^8$
g. $\frac{1}{4^{-8}}$ **h.** $\left(\frac{1}{4^4}\right)^{-2}$

3. Write each expression as a single power of p.
a. $(p^{-6})(p^{11})$ **b.** $((p^2)^3)^{-5}$
c. $\frac{(p^0)^4}{p^6}$ **d.** $\frac{(p^5)^0}{(p^0)(p^{-2})}$

4. Find each sum.
a. 3^0 **b.** $3^0 + 3^1$
c. $3^0 + 3^1 + 3^2$ **d.** $3^0 + 3^1 + 3^2 + 3^3$
e. $3^0 + 3^1 + 3^2 + 3^3 + 3^4$ **f.** What is the pattern of the results?

5. Write each number in scientific notation.
a. 1,000,000 **b.** 47,500 **c.** 512,000,000
d. 202,000 **e.** 0.00231 **f.** 0.00003579
g. $(4.1 \times 10^5)(4 \times 10^7)$ **h.** $(12 \times 10^3)(9 \times 10^4)$ **i.** 153,000 + 2,017,000

6. Write each number in decimal notation.
a. 2.53×10^5 **b.** 4.1032×10^{11} **c.** 1.59×10^{-5}
d. 4.72×10^{-8} **e.** 7.2×10^0 **f.** 5.06×10^{12}

7. Find the mean and median of each set of numbers.
a. 1.2×10^3, 3.4×10^4, 1.6×10^2, 9.8×10^3, 7.5×10^4
b. 3.21×10^4, 14.5×10^2, 28.2×10^3, 115×10^0, 228×10^3

8. Express each product or quotient in scientific notation.
a. $(5 \times 10^7)^3$ **b.** $(4 \times 10^9)^2$ **c.** $(6.2 \times 10^5)^2$
d. $\frac{6 \times 10^{12}}{3 \times 10^5}$ **e.** $\frac{9.3 \times 10^{11}}{3 \times 10^5}$ **f.** $\frac{5.2 \times 10^{10}}{4 \times 10^7}$

Practice: For Lesson 6.5, assign Exercises 5–8.

15. a. 8×10^{15} **b.** 1.4×10^{15}
c. 2.7×10^7 **d.** 6.25×10^8
e. $a^c \times 10^{bc}$

16. a. 3×10^8 **b.** 4×10^6
c. 1.6×10^5 **d.** 4×10^9

17. a. 4 **b.** 4.9 **c.** 4.95
d. 4.952 **e.** 4.9524 **f.** 4.95247
g. 4.952472
h. The powers of 10 give the place values for each number.

6.6 Getting Started

Activating Prior Knowledge
Exploring New Ideas

You will explore the relationship between square roots and squares.

For You to Explore

1. Explain how to locate each point on a number line.
   a. 7
   b. -5
   c. 101
   d. $\frac{3}{7}$
   e. $-\frac{5}{7}$
   f. $\frac{101}{7}$
2. There is only one positive number that satisfies the equation $\phi - 1 = \frac{1}{\phi}$. Based on this definition, find the value of ϕ.

You can pronounce the Greek letter ϕ as "fee" or "fy."

3. Follow these steps.
   - Choose an integer a.
   - Square the integer.
   - Find the prime factorization of the squared integer. How many twos are in the prime factorization?

   Repeat this process with at least five integers. Use even and odd integers.

   Is it possible to find an integer a, such that the prime factorization of a^2 contains an odd number of twos? If so, find the integer. If not, explain why.
4. Follow these steps.
   - Choose an integer b.
   - Square the integer.
   - Multiply the squared integer by 2.
   - Find the prime factorization of the result. How many twos are in the prime factorization?

   Repeat this process with at least five integers.

   In general, does the prime factorization of $2b^2$ contain an even or odd number of twos, or does it depend on your choice of integer b? Explain.
5. **Write About It** Can a perfect square ever be twice as large as another perfect square? Use your results from Problems 2 and 3 to explain.

Answers

For You to Explore

1. See back of book.
2. $\phi = \frac{1 + \sqrt{5}}{2} \approx 1.618$
3. No; squaring a number doubles the occurrence of each of its factors.
4. Any number built this way will have an odd number of twos in its prime factorization. From Exercise 3, you already know that a square number has an even number of twos in its prime factorization. Multiplying a square number by 2 will add a single two to the prime factorization.
5. No; a perfect square must have an even number of twos in its factorization, while a number that is twice as large as a perfect square must have an odd number of twos.

Lesson Overview

GOAL

- Warm up to the ideas of this investigation.

The results of For You to Explore Problems 3 and 4 in this lesson lay the groundwork for the proof that $\sqrt{2}$ is irrational. If students understand Problems 3 and 4, then the proof is surprisingly accessible.

FOR YOU TO EXPLORE
- Core: 1, 3, 4, 5
- Optional: 2

HOMEWORK
- Core: 6, 7, 8, 9, 10
- Optional: 11

Launch

Have your students work on For You to Explore Problem 2. Since ϕ is irrational, your students will not find the precise answer by refining approximations. You may quickly debrief after a few minutes of exploration. Then move onto Problem 3.

Explore

For You to Explore

PROBLEM 2 introduces irrational numbers. As students determine the precise decimal expansion of ϕ, or find a pattern in the decimal expansion, they may be surprised that it is not impossible. ϕ is a famous number, often referred to as the "golden mean." It appears in a number of different settings. For example, ϕ is the limit of the ratio of consecutive terms in the Fibonacci sequence. The Greeks believed rectangles with side length ratios of 1 to ϕ are the most aesthetically pleasing. You may wish to revisit ϕ once students learn the quadratic formula. They can use the quadratic formula to solve for ϕ directly because the equation $\phi - 1 = \frac{1}{\phi}$ is equivalent to the quadratic equation $\phi^2 - \phi - 1 = 0$.

PROBLEMS 3 AND 4 Students should complete these problems to help them understand the proof that $\sqrt{2}$ is irrational.

PROBLEM 5 previews the upcoming proof that $\sqrt{2}$ is irrational.

ERROR PREVENTION In Problem 5, watch out for students answering, "Yes, zero." That is not the intent of this question.

Wrap Up

Discuss For You to Explore Problem 5.

Exercises

HOMEWORK
- Core: 6, 7, 8, 9, 10
- Optional: 11

On Your Own

EXERCISE 7 lays the groundwork for describing the difference between rational and irrational numbers.

EXERCISE 8 introduces approximations of irrational numbers.

EXERCISE 9 You can never write an exact decimal expansion of $\sqrt{2}$. You can approximate $\sqrt{2}$ to any degree of accuracy that you desire by using the basic operations of arithmetic.

Maintain Your Skills

EXERCISES 10 AND 11 preview the definition of rational numbers and review basic moves of fractions and decimals.

Exercises *Practicing Habits of Mind*

On Your Own

6. Here is a list of perfect squares: 4, 9, 36, 49, 64, 100, 144, 400, 900. Find the prime factorization of each number. What do you notice about the factors?

7. Which of the prime factorizations represent numbers that are perfect squares? Which represent numbers that are not perfect squares? Try to find each result without calculating the product of the factors.

a. $a = 2^3 \cdot 3^2$ **b.** $b = 2^4 \cdot 3^2$ **c.** $c = 3^2 \cdot 5^2 \cdot 7$

d. $d = 3^2 \cdot 7^2$ **e.** $e = 5^2 \cdot 3^6$ **f.** $f = 2^5 \cdot 7^2 \cdot 5^2 \cdot 11^2$

8. Use this table to find the first two decimal places of $\sqrt{3}$. What kind of table would help you find the third decimal place of $\sqrt{3}$?

x	x^2	x	x^2
1.65	2.72	1.73	2.99
1.66	2.76	1.74	3.03
1.67	2.79	1.75	3.06
1.68	2.82	1.76	3.10
1.69	2.86	1.77	3.13
1.70	2.89	1.78	3.17
1.71	2.92	1.79	3.20
1.72	2.96	1.80	3.24

9. **Write About It** Suppose you have a calculator with only the four basic operations of arithmetic: $+$, $-$, $\times$, and $\div$. How can you use your calculator to find an approximation of $\sqrt{2}$?

Maintain Your Skills

10. Calculate each sum without using a calculator.

a. $\frac{1}{2} + \frac{1}{4}$ **b.** $\frac{1}{2} + \frac{1}{4} + \frac{1}{8}$

c. $\frac{1}{2} + \frac{1}{4} + \frac{1}{8} + \frac{1}{16}$ **d.** $\frac{1}{2} + \frac{1}{4} + \frac{1}{8} + \frac{1}{16} + \frac{1}{32}$

e. Describe a pattern in the results.

11. Express each sum as a fraction and as a decimal.

a. $\left(\frac{1}{1}\right)\left(\frac{1}{2}\right)$

b. $\left(\frac{1}{1}\right)\left(\frac{1}{2}\right) + \left(\frac{1}{2}\right)\left(\frac{1}{3}\right)$

c. $\left(\frac{1}{1}\right)\left(\frac{1}{2}\right) + \left(\frac{1}{2}\right)\left(\frac{1}{3}\right) + \left(\frac{1}{3}\right)\left(\frac{1}{4}\right)$

d. $\left(\frac{1}{1}\right)\left(\frac{1}{2}\right) + \left(\frac{1}{2}\right)\left(\frac{1}{3}\right) + \left(\frac{1}{3}\right)\left(\frac{1}{4}\right) + \left(\frac{1}{4}\right)\left(\frac{1}{5}\right)$

e. $\left(\frac{1}{1}\right)\left(\frac{1}{2}\right) + \left(\frac{1}{2}\right)\left(\frac{1}{3}\right) + \left(\frac{1}{3}\right)\left(\frac{1}{4}\right) + \left(\frac{1}{4}\right)\left(\frac{1}{5}\right) + \left(\frac{1}{5}\right)\left(\frac{1}{6}\right)$

f. Describe a pattern in the results.

Go Online Video Tutor
PHSchool.com
Web Code: bde-0775

Answers

6. 2^2, 3^2, $2^2 \cdot 3^2$, 7^2, 2^6, $2^2 \cdot 5^2$, $2^4 \cdot 3^2$, $2^4 \cdot 5^2$, $2^2 \cdot 3^2 \cdot 5^2$; all perfect squares have an even number of powers in their factorizations.

7. **a.** not a perfect square
b. perfect square
c. not a perfect square
d. perfect square
e. perfect square
f. not a perfect square

8. 1.73; to get more accuracy, you would need a table that break the intervel between 1.730 and 1.830 into thousandths.

9. Answers may vary. Sample: Test values by multiplying and build a table as in Exercise 8.

10. **a.** $\frac{3}{4}$ **b.** $\frac{7}{8}$
c. $\frac{15}{16}$ **d.** $\frac{31}{32}$
e. If the last fraction is $\frac{1}{n}$, the final sum equals $\frac{n-1}{n}$.

11. See back of book.

Power Ciphers

For a power cipher, the key will be the exponent. To encrypt with a given key, we raise the number to the keyth power and then reduce mod 26. The first question is whether or not this will work. For what keys will it work? For what mods? For purposes of understanding when a power makes a good cipher, we will first look at small mods even though they represent using alphabets that are much too small for good cryptography.

We need to have efficient and accurate ways to compute powers in modular arithmetic. We saw some efficient ways earlier.

Example: Encrypt with Power Cipher, Key = 5

plaintext:	p	o	w	e	r
encode:	15	*14*	*22*	*04*	*17*
CIPHERNUMBER:	19				

Encode "p" to get 15. Now compute 15^5 mod 5.

$15^5 \equiv 15^2 \cdot 15^2 \cdot 15 \pmod{26}$
$\equiv 225 \cdot 225 \cdot 15 \pmod{26}$
$\equiv 17 \cdot 17 \cdot 15 \equiv 4335 \pmod{26} \equiv 19$

Finish the encryption.

At this point to decrypt, we will make the entire power cipher table:

a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z
00	01	02	03	04	05	06	07	08	09	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25
00	*01*	*06*	*09*	*10*	*05*	*02*	*11*	*08*	*03*	*04*	*07*	*12*	*13*	*14*	*19*	*22*	*23*	*18*	*15*	*24*	*21*	*16*	*17*	*20*	*25*

Example:
Decrypt this message that was encrypted using Power Cipher, Key = 5

plaintext:	*c*	*i*	*p*	*h*	*e*	*r*
encode:	*02*	*08*	*15*	*07*	*04*	*17*
CIPHERNUMBER:	06	08	19	11	10	23

Do you think the inverse of a power cipher is also a power cipher? Do you think every power function will make a "good" cipher? The best way to investigate is to make tables. On the next page we will make the power table for mod 26. It is efficient to compute going down the columns.

Finding Patterns in Power Cipher Tables

The power cipher table for mod 26: To compute an entry in any column and row, take the number at the top of the column. Raise it to the exponent named for the row. Reduce mod 26.

Example: In row 3, we have
$1^3 = \pmod{26}$. $2^3 = 8 \pmod{26}$. $3^3 = 27 \equiv 1 \pmod{26}$. $4^3 = 64 \equiv 12 \pmod{26}$. etc.

power	Powers mod 26																								
1	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25
2				16																					
3	1	8	1	12																					
4				22																					
5				10																					
6																									
7																									
8																									
9																									
10																									
11																									
12																									
13																									
14																									
15																									
16																									
17																									
18																									
19																									
20																									
21																									
22																									
23																									
24																									
25																									

It is easier to compute the entire table by computing down the columns.

Example: Compute down the 4th column by repeated multiplying by 4, reducing as you go:

$1 \cdot 4 \equiv 4 \pmod{26}$
$4 \cdot 4 \equiv 16 \pmod{26}$
$16 \cdot 4 = 64 \equiv 12 \pmod{26}$
$12 \cdot 4 = 48 \equiv 22 \pmod{26}$
$22 \cdot 4 = 88 \equiv 10 \pmod{26}$
etc

1. Compute one of the other columns in the table. How far before you start repeating?

Notice some things about the table.

- The table is not symmetric about the diagonal as are multiplicative and additive tables. This is because the base and the exponent do not commute.

- The good ciphers are rows 1, 5, 7, 11

- The rows repeat with a period of 12.

- The 1st, 13th and 25th rows are identical and represent the identity cipher.

  Consequently, two keys will be inverses if their product is congruent to 1 mod 12. This is because $(m^k)^j=m^{kj}$. Understanding the repeating cycle is important in understanding the inverse of a power cipher.

- Each good cipher is it own inverse. Notice

  $5 \times 5 \equiv 1 \bmod 12$, so $(b^5)^5= b^{5\cdot5}= b^{2\cdot12+1}= b^{2\cdot12}\cdot b^1= (b^{12})^2\cdot b^1 \equiv (1)^2\cdot b = b$
  $7 \times 7 \equiv 1 \bmod 12$
  $11 \times 11 \equiv 1 \bmod 12$

  This will not always be true with other mods.

2. Make power cipher tables for the mods: 5, 6, 7, 8, 9, 10 11, 12, 13, 14, 15, 16, 17, 18 and answer these questions:

   a. What are the repeating patterns going down?
   b. Which rows make good ciphers?
   c. Find power inverses whenever possible.

What is observed:

- For prime numbers, the repeating pattern is always one less than the prime.

- For some mods, like 8, there are no good ciphers: the more factors in the mod the worse the case. If the mod, *m*, has a factor of p^2 (where *p* is a prime number) then the square of m/p (and hence the rest of the column) will be 0 mod *m*. So we need numbers that have no repeating prime factors.

Fermat's Little Theorem

The things we discover that worked mod 37, will in fact work for any prime modulus.

Fermat's Little Theorem:

If p is a prime number, then $a^{p-1} = 1 \pmod{p}$ for all a.

Why would this always be true? We have seen that this is true through the many examples we've done and used the fact that this also implies, by virtue of multiplying by a that

$$a^{p} = a \pmod{p}$$

These are exactly the two facts we need to show (as we did for the case $p = 37$) that the good power cipher keys mod p are all those numbers, n, that are relatively prime to p-1

Power Cipher Mod 37

First, we'll make an alphabet that has 37 letters. Then we will work mod 37. Since 37 is a prime number, we can make good use of power ciphers!

0	1	2	3	4	5	6	7	8	9	a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z	.
00	01	02	03	04	05	06	07	08	09	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31	32	33	34	35	36

Which powers make good ciphers? What is the inverse of a good power cipher mod 37?

We will proceed by assuming we know that there is an inverse for the power cipher, say key = n and see what we can learn about n and a possible inverse for the power cipher. Suppose that the inverse is also a power cipher. What would that look like? We see from the tables that the power cipher key=37 is the identity or

$$a^{37} = a \pmod{37} \text{ for all } a. \qquad \textit{(fact 1)}$$

(this, by the way, makes 37 a "good" key because the inverse of the identity is the identity)

$$a^{36} = 1 \pmod{37} \text{ for all } a. \qquad \textit{(fact 2)}$$

(this, by the way, makes 36 a "bad" key because a constant function is not 1-1.)

Suppose that the power cipher, m, were the inverse of power cipher, key n. Then raising to the nth power followed by raising to the mth power would get you right back to where you started, in algebraic language:

$$(a^n)^m = a \pmod{37}$$

this would be true if $nm = 1$. By virtue of ***fact 1***, it would also be true if $nm = 37 = 1+36$. By ***fact 2***, multiplying by a^{36} is like multiplying by 1 mod 37. We can also deduce the statement is true if $nm = 1 + 2 \cdot 36$ or, in general, if

$$nm = 1 \pmod{36}$$

The inverse power mod 37 for a key n, is the multiplicative inverse of n mod 36.

Because of what we know about multiplicative inverse mod 37, the good power keys mod 37 are just those numbers, n, that are relatively prime to 36.

By virtue of Fermat's Theorem, the same is true for any prime mod.

Examples: Use a power cipher mod 37 with key = 7 to encrypt the following message:

```
 c   a   n   d   y
12  10  23  13  34
09  10  14  32  33
```

The multiplicative inverse of 7 mod 36 is 31 (we know many ways to compute it) because 7*31 = 217 (36*6+1) ≡ 1 mod 36.

To check that this is right, use the power 31 mod 37 to decrypt: 09 10 14 32 33

1. Pick another good power cipher key mod 37 and encrypt your name.

Power Cipher Mod p·q
when p and q are prime numbers

The good ciphers mod p·q are those powers that are relatively prime to (p-1)·(q-1)

The power inverse of the power *n* is the multiplicative inverse of *n* mod (p-1)·(q-1)

Example: Power Cipher Mod 55

The good ciphers mod 55 are those powers that are relatively prime to 40, because 55 = 5·11 and (5-1)·(11-1) = 4·10 = 40. So the good ciphers are

1, 3, 7, 9, 11, 13, 17, 19, 21, 23, 27, 29, 31, 33, 37, 39

1. Find the power inverse of 13, use any form of the Extended Euclidean algorithm to solve:

$$13 \times \square \equiv 1 \mod 40$$

inverse is 37

Use the regular letter to number code for the 26-letter alphabet to do the following problems

2. Encrypt mod 55, using the power cipher 13:

P	O	W	E	R
15	14	22	04	17
20	49	22	09	17

3. Test that that to decrypt a message that was encrypted with a power cipher key 13, you the power 31. For example, $20^{31} \equiv 15 \mod 55$

4. Decrypt this word that was encrypted using the power cipher 29:

C	I	P	H	E	R
02	08	15	07	04	17
17	18	25	52	14	02

Notice: We could use any numbers from 0 to 54 in our encryption scheme. If we just use the 26 letters our encryptions may contain numbers large than 26 so we can not decode back to letters.

Power Cipher Mod 437

437 = 23·19 The good ciphers mod 437 are those powers that are relatively prime to 22·18 = 396, because 55 = 5·11 and (5-1)·(11-1) = 4·10 = 40.

1. List ten numbers that are relatively prime to 396:

Notice: any prime number that is not a factor of 396 is relatively prime to 396.

Example: Consider the power cipher, key 47

The inverse of 47 mod 396 is 59.

[Confirm that 47· 59 = 2773 = 7· 396 + 1]

2. Find the inverses mod 396 of the five of the numbers you listed in 1.

3. Use the power cipher 47 to encrypt the letters:

P	O	W	E	R
15	14	22	04	17
155	260	390	225	175

4. Check the work by raising each cipher number to the 59th power:

$155^{59} \equiv 15 \mod 437$
$260^{59} \equiv 14 \mod 437$
$390^{59} \equiv 22 \mod 437$
$225^{59} \equiv 4 \mod 437$
$175^{59} \equiv 17 \mod 437$

5. Make our own power cipher mod 437. Make sure you know how to encrypt and decrypt. Encrypt a four letter secret password.

Power Ciphers: Using Larger Mods

In this project you will make your own power cipher from scratch. You will choose you modulus that is the power of two primes: **n = p·q** You will choose a number, **e**, that is relatively prime to **(p-1)·(q-1)**. You will find the inverse of **e** mod **(p-1)·(q-1)**.

Pick two prime numbers. Both should be larger than 50. Call them **p** and **q**.

p = _____

q = _____

n = p·q = _____

(p-1)·(q-1) = _____

Find a number, call it **e**, that is relatively prime to **(p-1)·(q-1)**.

e = _____

Find the inverse of e, $\mathbf{e^{-1}}$ mod (p-1)·(q-1).

$\mathbf{e^{-1}}$ = _____

1. To check your work, do the following

   Compute 4^{e}. Answer = _____

   Take the Answer and raise it to the power $\mathbf{e^{-1}}$. Answer = _____

2. Think of a good four-letter password. Encrypt it with your power cipher. Check your work raising each number in your encryption to the $\mathbf{e^{-1}}$.

letters:				
encode:				
encrypt:				

   Write the encrypted numbers on a 3 x 5 card. Write your values for **n** and **e** on the back of the card.

Power Ciphers: RSA Encryption

RSA Encryption is a power cipher that uses a two prime numbers that are so large that it is impossible, uisng current computer technology, to determine if the product is a prime or not. (Unless, of course, you know the two prime numbers to start.) This means that the encrypter can tell anyone what modulus, ***n***, is used using and what power, ***e***, is used. Because one can not find the inverse of **e**, without knowing the two prime numbers,

Besides being almost impossible to crack RSA has another advantage. Anyone who knows your key can encrypt a message, but only those who know the inverse can decrypt that message. This makes it valuable for computer security application. You tell the whole world your public key and they can send you messages protected from listening ears but only you can decrypt the message when it is safely on your computer.

Make your own private key:

Pick two prime numbers. Both should be larger than 100 so that the product of the two is larger than 10,000. Call them **p** and **q**.

p = _____

q = _____

n = p·q = _____

(p-1)·(q-1) = _____

Find a number, call it **e**, that is relatively prime to **(p-1)·(q-1)**.

e = _____ (**n**,**e**) is called your *pubic key*.

Find e^{-1} mod $(p\text{-}1)\cdot(q\text{-}1)$.

$\mathbf{e^{-1}}$ = _____ $\mathbf{e^{-1}}$ is yoru private key

1. To check your work, do the following

   Compute 4^{e}. Answer = _____

2. Take the Answer and raise it to the power $\mathbf{e^{-1}}$. Answer = _____
   (If your answer is not 4, try again.)

3. Put your private key into the class directory of public keys. Remember your private key but don't tell it to anyone.