

Number Theory

For Teachers

Interactive Notes

Bonnie Saunders, 2012



Number Theory for Teachers, Interactive Notes by [Bonnie Saunders](#) is licensed under a [Creative Commons Attribution-NonCommercial-ShareAlike 4.0 International License](#).

How to use this book:

These pages are designed as an *interactive workbook*. This means that we will be reading and discussing the text in class. We will be also working on the problems together. It may be difficult to complete problems on your own before there has been class discussion.

1 Crickets

Numberline Arithmetic with Negative Numbers
Why is a negative times a negative a positive?


Crickets and Arithmetic Sequences
Writing Formulas and Equations


Crickets: Other Problems

following

*Additive Ciphers
and Maneuvers on Number Lines*

Crickets: Numberline 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:

$$-1 + 3 \times 2 = 5$$



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

$$3 + 2 \times -2 = -1$$



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

$$-4 - 2 \times -5 = 6$$



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. $3 - 2 \times 4 =$



9. $-3 + 4 \times 2 =$



10. $0 - 4 \times -3 =$



Question: What is the difference between the expression

-4×-3 (multiplying the inverse of four times the inverse of 3)

and the expression

$0 - (4 \times -3)$ (subtracting 4 times the inverse of 3 from 0) ?

Some people use the cricket model to show that a negative number times a negative number is a positive number. They would say that -4×-3 means “ a -3 cricket going backwards 4 jumps” and so must be the same as 4×3 . To others this is unsatisfactory because then -4 takes on a different role than -3 and, because when talking about cricket movements, we also need to say where the cricket starts. Therefore the proper expression to represent is $0 - (4 \times -3)$ and doesn't really tell us about a negative number times another negative number.

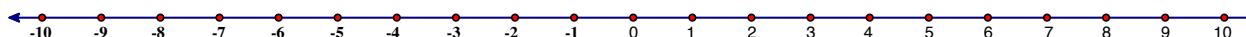
Understanding the differences between the two expressions and understanding that they represent the same number is an algebra exercise.

Why is a negative times a negative a positive?

On this page we will show how we can understand that $-3 \times -4 = 3 \times 4$. This will allow us to say that $-a \times -b = a \times b$ for any positive numbers a and b , because our argument will be easily seen to work for any two numbers, not just 4 and 3. We take advantage of well-known patterns we see from working with negative numbers on the number line. **We proceed in two steps.**

Step 1: We will convince ourselves that a positive number times a negative number should be a negative number, by showing that $4 \times (-3) = -(4 \times 3) = -12$.

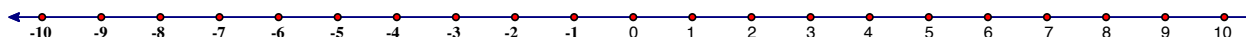
Start with the known arithmetic facts about multiplying that 4×3 and observe the following number pattern that we construct using multiplication facts we know about positive integers and what we know about negative numbers on a number line:



$4 \times 3 =$	12
$4 \times 2 =$	8
$4 \times 1 =$	4
$4 \times 0 =$	0
$4 \times -1 =$	-4
$4 \times -2 =$	-8
$4 \times -3 =$	-12

We start this table by filling in the multiplication facts we already know from looking at a +4 cricket jumping from 0.

Thinking about this cricket moving backwards convinces us that, as we decrease the multiplier: 3 2 1 0 -1 -2 -3, the cricket lands on 12 8 4 and then 0 -4 -8 -12. This comes from our understanding of patterns created by crickets. We stop the exact number of steps to the left of 0 as we started on the right, so we naturally land on the opposite of where we started: $4 \times -3 = -(4 \times 3) = -12$



Step 2: Confident that a positive number times a negative number is a negative number, we will convince ourselves that $-3 \times -4 = 12$. This time we consider the -4 cricket.

$3 \times -4 =$	-12
$2 \times -4 =$	-8
$1 \times -4 =$	-4
$0 \times -4 =$	0
$-1 \times -4 =$	4
$-2 \times -4 =$	8
$-3 \times -4 =$	12

We start this table by filling in the multiplication facts we learned in the first step. We recognize the pattern -8 -4 will continue to 0 4 8 12 as the cricket jumps backwards and the multiplier changes 2 1 0 -1 -2 -3

We know the cricket continues up the number line, moving up 4 spaces every jump. So after going 4 jumps past zero, he lands on 12: $-3 \times -4 = 12$

1. Draw the number line that shows the movements of the -4 cricket in **Step 2**.

2. Repeat this procedure with another set of numbers. For example, show that $-7 \times -5 = 35$

Crickets and Arithmetic Sequences

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

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

$$2, 5, 8, 11, 14, 17, \dots$$

The starting number is 2; the difference number is the same as the cricket number, +3.

A formula for the $(n+1)$ th number in the sequence is given by $2+3 \cdot n$. When $n = 0$ the cricket is on the first number, 2. After the first jump ($n = 1$) the cricket is on 5, after the second jump ($n = 2$) the cricket is on 8, etc.

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

$$18, 13, 8, 3, -2, -7, -12, \dots$$

A formula for this arithmetic sequence would be $18 - 5n$, the $(n+1)$ th number on the list. 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*.

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 like an arithmetic sequence in both directions.

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

$$\dots -13, -10, -7, -4, -1, 2, 5, 8, 11, 14, 17, \dots$$

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

$15, 11, 7, 3, -1, -5, -9, \dots 15 - 4n$, where n is the number of jumps

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

$\dots, -11, -4, 3, 10, 17, 24 \dots 3 + 7n$, where n is the number of jumps from 3.

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.
 $7n - 9$
2. If a -9 cricket starts on 7, write a formula for where he lands on his n^{th} jump.
 $7 - 9n$
3. 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.
 $103 - 17n = 2$
4. What kind of crickets could make these jumps? Fill in the rest of the landing numbers.

$$\begin{array}{l} \phantom{6+19n = nth \text{ jump after } 6} \\ +19: (82-6)/4 = 19; 6+19n = nth \text{ jump after } 6 \\ -19: (6-82)/4 = -19; 82-19n = nth \text{ jump after } 82 \end{array}$$

Try another one:

$$\begin{array}{l} \phantom{-113+22n = nth \text{ jump after } -113} \\ +22: (19-(-113))/6 = 22; -113+22n = nth \text{ jump after } -113 \\ -22: (-113-19)/6 = -22; 19-22n = nth \text{ jump after } 19 \end{array}$$

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.

Cricket: Other Problems

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.

start on 16 jump 7 times: $23n + x = 177$

Division Algorithm

For each of the following problems:

- Solve in a simple-minded, tedious manner.
 - Show a more efficient way to solve the problem.
 - Explain how to think about these problems as cricket problems.
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?
 3. Larry and Mary bought a special 360-day joint membership to a tennis club, 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?

2 *Substitution Ciphers*

Simple Substitution Cipher
Tables for Encrypting and Decrypting
Counting: How many Ciphers Tables are there?
Studying Big Numbers

Cryptography in Spanish: Frequency Analysis

Guess the Keyword 1
Guess the Keyword 2

following
Keyword and other Substitution Ciphers

Simple Substitution Cipher

In a simple substitution cipher, each letter of the alphabet is replaced by another letter. There may be a pattern, like with a Caesar Cipher, but there doesn't need to be one. The letters may be scrambled up in any order.

Example: Here is a cipher table for a substitution cipher that has no obvious pattern.

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
D	X	M	E	Z	W	V	F	L	A	N	K	G	O	B	U	P	T	J	H	C	S	Q	I	Y	R

1. Use the table to encrypt and decrypt.

c	i	p	h	e	r
M	L	U	F	Z	T

t	a	b	l	e
H	D	X	K	Z

2. Make your own simple substitution cipher in this 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

3. Describe how you made sure that every letter appeared only once in the second row of your cipher table.

4. Write a message and encrypt it using your cipher. Give the encrypted message to a friend and see if they can decrypt it.

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. encrypting 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
F	D	A	V	S	M	Q	C	T	X	U	K	W	P	Y	Z	G	L	E	O	N	J	B	H	R	I

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

Encrypt					
c	i	p	h	e	r
A	T	Z	C	S	L

Decrypt					
t	a	b	l	e	s
O	F	B	K	S	E

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

Table II, Decrypting Table

c	w	h	b	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						
a	r	e		f	u	n
F	L	S		M	N	P

Decrypt					
t	o		u	s	e
O	Y		N	E	S

It doesn't make any difference which table you use to encrypt or decrypt. In both cases the plaintext "a" encrypts to ciphertext "F", plaintext "b" encrypts to "D", and so on. In both cases that ciphertext "A" decrypts to plaintext "c", ciphertext "B" decrypts to plaintext "w", and so on.

It may make a difference for some people in how easy it is encrypt or decrypt messages.

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

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

7. Which 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 how to get it.

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

We want to make "good" ciphers. So we don't want any two different plaintext letters to encrypt to the same ciphertext letter. And we 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 one make using an alphabet of just two letters?

a	b
A	B

a	b
B	A

ANSWER: 2

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

a	b	c
A	B	C

a	b	c
A	C	B

a	b	c
B	A	C

a	b	c
B	C	A

a	b	c
C	A	B

a	b	c
C	B	A

ANSWER: $3 \times 2 = 6$ or 3 letters go with "a" times 2 ways to assign the other 2 numbers.

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!

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

ANSWER: $4 \times 6 = 24$ or 4 letters go with "a" times 6 ways to assign the other 3 letters.

What is the pattern? Can you write a formula for the number of different cipher table for an alphabet with n letters? Always n times previous number of ways, so n! – see table.

Studying Big Numbers

Explore with numbers to help students understand exactly how big is the number

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

1. Write the number in scientific notation with 3 significant figures.

4.03×10^{26}

2. If this number were a number of seconds, how many years would it represent?
3. If this number were a number of miles how many round trips to the moon would it represent?
4. If this number were a number of living cells, how many human beings would it represent?

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 .

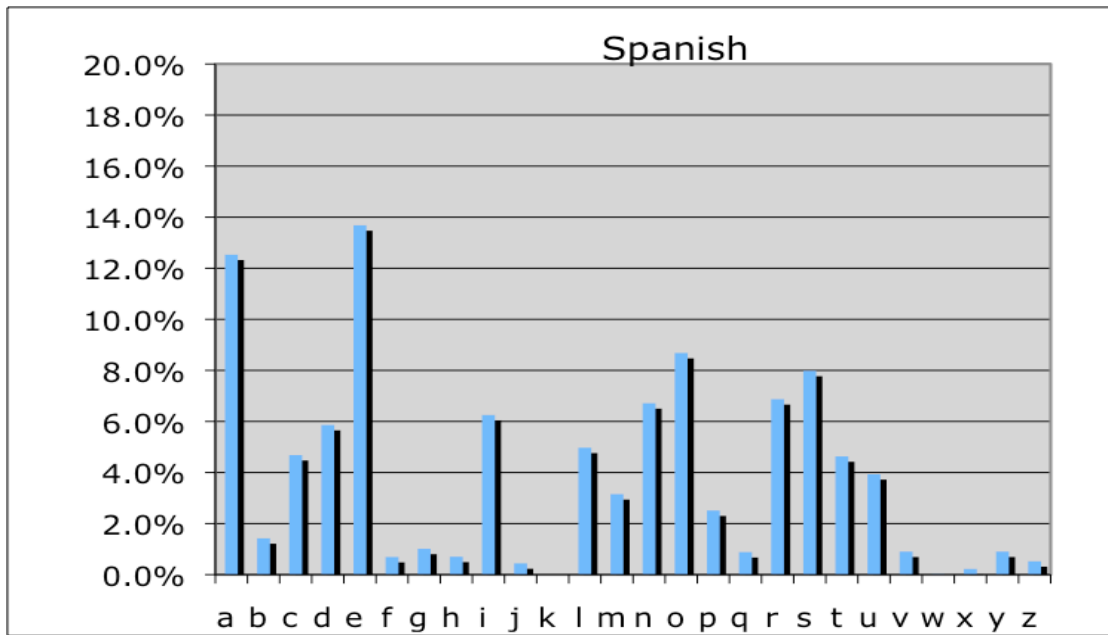
key=11, most common Z (o) 13.5%

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 1

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
Q	S	T	U	V	W	X	Y	Z	P	R	I	M	E	A	B	C	D	F	G	H	J	K	L	N	O

GYVDV ZF EA QBBQDVEG DVQFAE KYN

AEV EHMSVD ZF BDZMV QEU QEAGYVD

EAG. GA GYV TAEGDQDN, HBAE

IAARZEX QG GYV FV EHMSVDF AEV

YQF GYV WV VIZEX AW SVZEX ZE GYV

BDV FVETV AW AEV AW GYV

ZEVLBI ZTQSIV FVT DVGF AW TDVQGZAE. -

U. OQXZVD

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

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
keyword=PRIME, keyletter=j

Guess the Keyword 2

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
S	V	W	X	Z	N	U	M	B	E	R	T	H	O	Y	A	C	D	F	G	I	J	K	L	P	Q

GMZ ADYVTZH YN XBFGBOUIBFMBOU

ADBHZ OIHVZDF NDYH WYHAYFBGZ

OIHVZDF SOX YN DZFYTJBOU GMZ

TSGGZD BOGY GMZBD ADBHZ NSWGYDF

BF ROYKO GY VZ YOZ YN GMZ HYFG

BHAYDGSOG SOX IFZNIT BO

SDBGMHZGBW. -- 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

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
Keyword=NUMBERTHEORY keyletter=f

3 *Combination Charts*

Problems and Algorithms

Combination Charts

Combination Chart Problems

Combination Problems

Problems with Negative Combinations

following

MIC Combination Problems and Crickets

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

$$n \times (\text{the number of steps to the right from } 0) + m \times (\text{the number of steps up from } 0)$$

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 combination 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: $25 = 5 \times 3 + 2 \times 5$ $-12 = 1 \times 3 + (-3) \times 5$
 $1 = (-3) \times 3 + 2 \times 5$ $-22 = (-4) \times 3 + (-2) \times 5$

Arrows: We use arrows to talk about moving about on a combination chart. \rightarrow means move one unit to the right. \uparrow means move one unit up. \leftarrow means move one unit to the left. \downarrow means move one unit down.

Introduce this page with examples of combination problems that use need negative number solutions: Solving $x \equiv 2 \pmod{5}$, $x \equiv 1 \pmod{3}$. And weighing 4oz using 3oz and 5oz weights.

Cricket: 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 $\rightarrow\uparrow$ 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 $\rightarrow\uparrow\uparrow$ cricket starting on a -21 on the 3,5 Combination Chart will jump out the sequence

$$-20, -7, 6, 19, 32, \dots$$

adding $+13 = 3 + 2 \times 5$ (3 for the \rightarrow and 5 for each \uparrow) with each jump. If the same cricket starts on a -6 it hops out the sequence

$$-6, 2, 15, 28, 41, \dots$$

still adding $+13$ with each jump. Notice a formula for this cricket's jumps is $-6 + 8n$, 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, \dots : all even numbers.
2. Describe with arrows the cricket on the 3,5 combination chart that jumps out the sequence 9, 23, 37, \dots : $9 + 17n$, where n is number of jumps since 9.
3. Write a formula for a $\uparrow\leftarrow\leftarrow$ 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 $\rightarrow\rightarrow\uparrow$ 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.

$\leftarrow\leftarrow\leftarrow\uparrow\uparrow\uparrow = \leftarrow^4\uparrow^3$ is one way. NOTE: $12 + 6\cdot(-4)+8\cdot4 = 12$

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.

$+22 \rightarrow\rightarrow\uparrow\uparrow\uparrow\uparrow = 2\cdot1+4\cdot5$

$+38 \rightarrow\rightarrow\rightarrow\uparrow\uparrow\uparrow\uparrow\uparrow\uparrow = 3\cdot1 + 6\cdot5$

$-24 \leftarrow\leftarrow\leftarrow\downarrow\downarrow\downarrow = -4\cdot1 + (-4)\cdot5$ or $\downarrow\downarrow\downarrow\downarrow\rightarrow = 1 + (-5)\cdot5$

For any number, divide by 5. The quotient is the number of \uparrow and the remainder is the number of \rightarrow

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?

$\rightarrow\rightarrow\downarrow = 2\cdot4+(-1)\cdot7 = +1$

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.

$$m \times n - n \times m = 0.$$

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 \rightarrow and y be amount of \downarrow 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:

Combination Problems

Make combination charts to help solve or illustrate each of these 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 17 heads and 44 legs among the chickens and dogs on his farm. How many dogs and how many chickens does he have?

Find all of the 44's on a 2,4 combination chart

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?

Better to ignore the combination chart and realize that 286 is not a multiple of 3

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?

It really helps to look at the combination chart to see why every amount greater than 47 is a combination of 5 and 13.

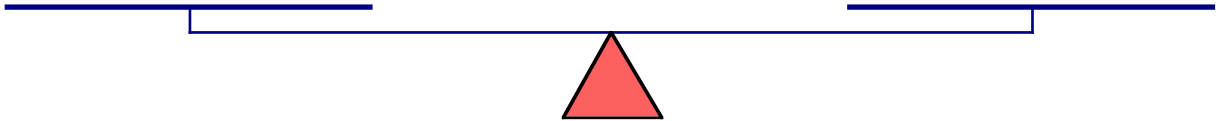
5. **Challenge:** I only have 31¢ and 37¢ stamps. What is the largest postage that cannot be made using only these stamps?

Problems with Negative Combinations

Make combination charts to illustrate solutions to these problems. We will need to show negative combinations.

1. 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?

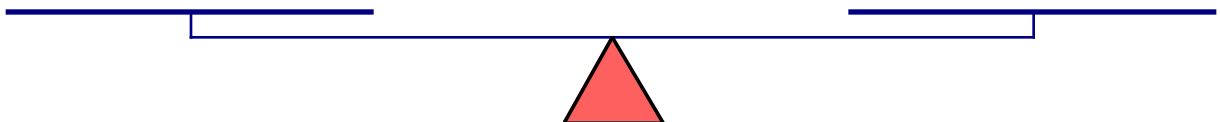
Notice: once you can get the 1 oz you know you can get any amount.



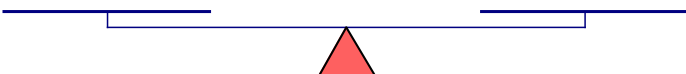
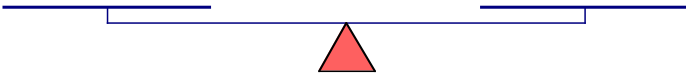
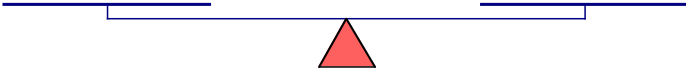
To solve analytically, we need to solve $5m - 3n = 1$ for positive values m, n . So we are solving $5m + 3(N) = 1$ for m positive and N negative. More generally, we solve $5M + 3N = 1$ for solutions M, N where one is positive and one negative.

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

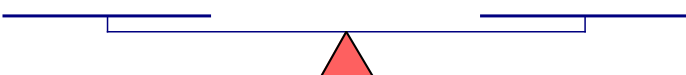
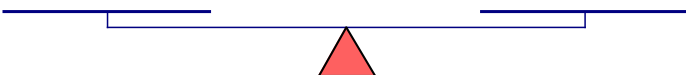
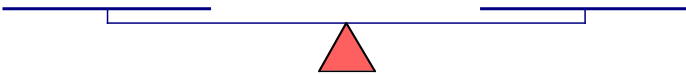
$\gcd(12, 15) = 3$. Every weight you can determine must be a multiple of 3 because both of your weights are. Once you can get 3 oz. (which is possible) you can get any multiple of 3.



o



o



4 *More on Algebra*

Arithmetic and Algebra

Some Definitions and previous notions

Basic Rules of Algebra

Basic Rules for Equations

Identifying Identities

The Division Algorithm

Special Case $r = 0$

following
Multiplicative Ciphers

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

$a \times b$ 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 Algebra

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 <i>nonzero</i> number a , there is a 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 , $a \cdot (b + c) = a \cdot b + a \cdot c$
----------------------------	---

Notice that the rules of algebra say nothing about subtraction or division, except to mention the existence of inverse operations. 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: *the inverse of additive*

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 allows subtracting larger numbers from smaller numbers.

Meaning of division: *the inverse of multiplication*

Dividing a by b from is like multiplying a by the multiplicative inverse of b .

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

Note that this way of thinking about division gives meaning to fractions, even when numerator and denominator are not whole numbers:

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

1. Use the Basic Rules of Arithmetic and this new meaning for subtraction to show that these statements are true.

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

First, commute a and $(b+c)$, then distribute a across $b+c$, then commute again.

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

First, change $b - c$ to $(b + -c)$, then distribute a , then change back to subtraction.

c. For any numbers a , b , c , and d , $(a + b) + (d + c) = a + (b + (d + c))$

Here are some fun problems to think about:

2. How many different ways can you put parentheses on $a + b + c + d$?

3. How many different ways can you find $3 + 4 + 6 + 5$?

Basic Rules for Equations

In Algebra you learned about solving equations by understanding all the ways you can change an equation without changing the solution(s) to the 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)

Example: Solve the equation, $3x + 7 = 22$. Explain every step.

result	justification
given: $3x + 7 = 22$	
$(3x + 7) + -7 = 22 + -7$	add same number (-7) to both sides
$3x + (7 + -7) = 22 + -7$	apply associative addition rule
$3x + (7 + -7) = 15$	arithmetic fact ($22 + -7 = 15$)
$3x + 0 = 15$	use additive inverses ($7 + -7 = 0$)
$3x = 15$	use additive identity $3x + 0 = 3x$
$3^{-1}(3x) = 3^{-1} \cdot 15$	multiplying both sides by same number (in this case 3^{-1})
$(3^{-1} \cdot 3)x = 3^{-1} \cdot 15$	apply associative multiplication rule
$(3^{-1} \cdot 3)x = 5$	arithmetic fact ($3^{-1} \cdot 15 = 5$)
$1 \cdot x = 5$	use multiplicative inverses ($3^{-1} \cdot 3 = 1$)
$x = 5$	use multiplicative identity

Finally, we need to check to see if the answer is correct: $3 \cdot 5 + 7 = 15 + 7 = 22$ ✓

1. Solve the following equation, $8 - x = 2x + 6$. Explain every step.

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

2. $2(a \cdot b) = (2a \cdot 2b)$

3. $4(a \cdot b) = (2a \cdot 2b)$

4. $(a + b)^2 = a^2 + 2a \cdot b + b^2$

5. $(a + b)^2 = a^2 + b^2$

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

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:

Example 1: 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?

$$531 \div 25 = 41 \text{ R } 6 \text{ or } 531 = 25 \cdot 40 + 6$$

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.

$$\begin{array}{r} 131 \\ -23 \quad 1 \\ \hline 108 \\ -23 \quad 2 \\ \hline 85 \\ -23 \quad 3 \\ \hline 62 \\ -23 \quad 4 \\ \hline 39 \\ -23 \quad 5 \leftarrow q \\ \hline 16 \quad \leftarrow r \end{array}$$

Example 2: What is the smallest positive number that a +23 cricket would start on in order to eventually land on 131? How many jumps would it take to get there?

Solve this problem by working backwards: the +23 cricket starts at 131 and goes backward, subtracting 23 each jump until it can't go further without passing 0. This is done at the right and shows that

$$131 = 23 \cdot 5 + 16 \quad (m = 131; n = 23; q = 5, r = 16)$$

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.

Example 3: What is the smallest positive number that a +23 cricket, starting on -177, will get to? How many jumps would it take to get there?

Solve this problem by working backwards from -131: the +23 cricket starts at -131 and goes forward, *adding* 23 each jump until it passes 0. This is done at the right (The jumps are counted as negative numbers because, to work from the answer to -131 a positive cricket goes backwards) and shows that

$$-131 = 23 \cdot (-6) + 7 \quad (m = -131; n = 23; q = -6, r = 7)$$

$$\begin{array}{r} -131 \\ +23 \quad -1 \\ \hline -108 \\ +23 \quad -2 \\ \hline -85 \\ +23 \quad -3 \\ \hline -62 \\ +23 \quad -4 \\ \hline -39 \\ +23 \quad -5 \\ \hline -16 \\ +23 \quad -6 \leftarrow q \\ \hline 7 \quad \leftarrow r \end{array}$$

Using division: We can always find q and r by dividing m by n and then figuring a positive remainder. Care must be taken with negative numbers, the quotient may change.

Example 4: For $m = 60$, $n = 7$, $q = 8$ and $r = 4$.
because $60 = 8 \cdot (7) + 4$

For $m = -60$, $n = 7$, $q = -9$ and $r = 3$.
because $-60 = -9 \cdot 7 + 3$

In the context of cryptography and modular arithmetic, the divisor, n , will always be positive. However, it is good to see that the Division Algorithm works even if the divisor is negative:

Example 5: For $m = 60$, $n = -7$, $q = -8$ and $r = 4$.
because $60 = -8 \cdot (-7) + 4$

For $m = -60$, $n = -7$, $q = 9$ and $r = 3$.
because $-60 = 9 \cdot (-7) + 3$

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

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

$$q = 41 \text{ and } r = 0 \quad 124 = 41 \cdot 4 + 0$$

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

$$q = -5 \text{ and } r = 8 \quad -100 = -5 \cdot 23 + 15$$

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

$$q = -15 \text{ and } r = 1 \quad 104 = -15 \cdot (-7) + 1$$

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

$$q = -21 \text{ and } r = 5 \quad -215 = -21 \cdot (-10) + 5$$

Finding remainders using a calculator

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

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 a *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 a *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: $n|m$

NOTE: $n|m$ 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 .

1. Which of the following statements are true? Which are false? Explain.

a. $24 | 4$

f. 21 is a multiple of 7.

b. $4 | 24$

g. Any non-zero number divides 0.

c. $7 | 48$

h. Zero is a multiple of any number.

d. For any two integers p and n , $p|p \cdot n$

i. Zero divides 3.

e. 21 is a factor of 7

j. There are four numbers that divide 3.

2. List all divisors of 48.

5 *GCD and LCM*

Factors: Definitions and Examples

GCD and problems

LCM and Problems

Cricket and Chinese Remainders

Finding the GCD without factoring

The Euclidean Algorithm

Practice with the Euclidean Algorithm

Geometry and the Euclidean Algorithm

following

*Multiplicative Ciphers
and Cricket*

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 $15 = 5 \times 3$.

We also say, “5 divides 15” and 5 is a divisor of 15.

6 is not a factor (or divisor) of 15 because $15 \div 6 = 2 \text{ R } 3$.

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-negative numbers is the greatest integer that divides all of the numbers. The greatest common divisor of two non-negative integers A and B is abbreviated by $\text{gcd}(A, B)$. 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

common factors of 168 and 154: 1, 2, 7, 14

$\text{GCD}(168, 154) = 14$

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've done everything required by the definition.

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

$612 = 2^2 \cdot 3^2 \cdot 17$

$132 = 2^2 \cdot 3 \cdot 11$

$180 = 2^2 \cdot 3^2 \cdot 5$

greatest power of 2 is 2; greatest power of 3 is 2;

there are no other common prime factors.

so $\text{GCD}(612, 132, 180) = 2^2 \cdot 3 = 12$

Why does this work? Clearly, our answer is a common divisor (a factor of all 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 been included in our answer.

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

Practice Problems:

1. $\text{gcd}(322, 21)$

$\text{gcd}(90, 45, 33)$

$\text{gcd}(625, 102)$

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. The squares must exactly tessellate the area. What is the largest square pattern you could use?

3. Which keys are good multiplicative keys?

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 $(612/12) \cdot 132 = 51 \cdot 132$, a multiple of 132. or $(132/12) \cdot 612 = 11 \cdot 612$, 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.

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?
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?
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?
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?

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. **Challenge:** 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.

$$\gcd(64,62) =$$

$$\gcd(51, 54) =$$

$$\gcd(175,170) =$$

$$\gcd(175,165) =$$

$$\gcd(51, 57) =$$

$$\gcd(64,70) =$$

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 $a > b$, $\gcd(a, b) = \gcd(b, a - b)$

$$\gcd(55,25) =$$

$$\gcd(75,30) =$$

$$\gcd(175,75) =$$

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 such that $a > n \cdot b$, $\gcd(a, b) = \gcd(b, a - n \cdot b)$

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 non-negative 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:

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

Example: Compute $\gcd(138, 120)$.

because $138 - 1 \times 120 = 18$,	by Fact 2, we know that $\gcd(138, 120) = \gcd(120, 18)$
because $120 - 6 \times 18 = 12$,	by Fact 2, we know that $\gcd(120, 18) = \gcd(18, 12)$ ¹
because $18 - 1 \times 12 = 6$,	by Fact 2, we know that $\gcd(18, 12) = \gcd(12, 6)$
because $12 - 2 \times 6 = 0$,	by Fact 2, 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 $\gcd(165, 76)$. You write the justifications

$165 - 2 \times 76 = 13$
 $76 - 5 \times 13 = 11$
 $13 - 1 \times 11 = 2$
 $11 - 5 \times 2 = 1$
 $2 - 2 \times 1 = 0 \leftarrow$ 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:

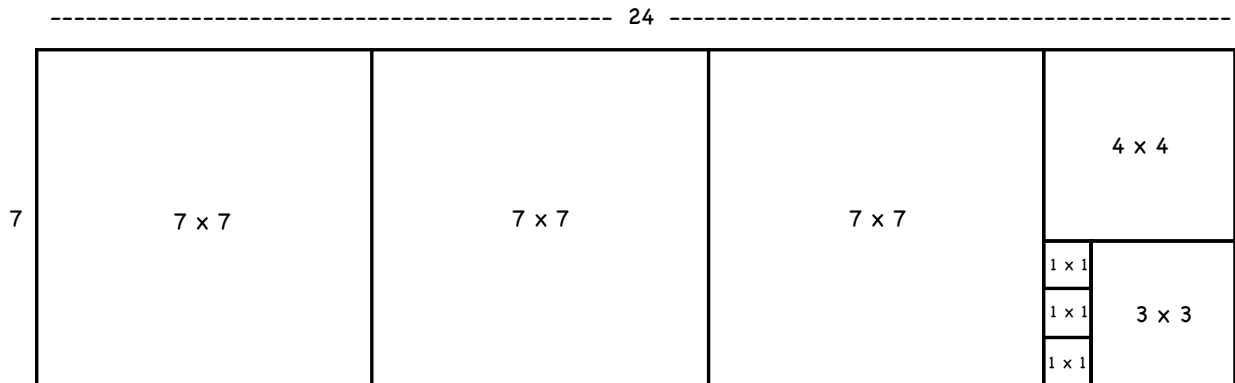
1. Write down all divisors of each number, circle the common ones, then locate the largest common one.
2. Write each one as a product of prime factors. Use the results to write the gcd as a product of primes.

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 24×7 rectangle exactly



6 *Extended Euclidean Algorithm*

Problems and Algorithms

The Extended Euclidean Algorithm: Solving
 $A \cdot x + B \cdot y = \gcd(A, B)$
More Diophantine Equations to Solve

Optional

Finding Multiplicative Inverses
Extended Euclidean Algorithm Worksheet
TI-84 Program for finding $\gcd(A, B)$ and solutions
to $Ax + By = \gcd(A, B)$

following

*MIC Combination Problems
and Crickets*

The Extended Euclidean Algorithm: 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. *Throughout x and y are integers – possibly negative.*

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:

$$\begin{array}{llll}
 11 - 3 \cdot 3 = 2 & = \uparrow \leftarrow \leftarrow \leftarrow & = \uparrow \leftarrow^3 & \text{or } 11 \cdot (1) + 3 \cdot (-3) = 2 \\
 3 - 1 \cdot 2 = 1 & = \rightarrow \downarrow \rightarrow \rightarrow \rightarrow & = \downarrow \rightarrow^4 & \text{or } 11 \cdot (-1) + 3 \cdot 4 = 1 \leftarrow \\
 2 - 2 \cdot 1 = 0 & = \uparrow \leftarrow^2 - 2(\downarrow \rightarrow^4) & = \uparrow \leftarrow^3 \leftarrow^{11} & \text{or } 11 \cdot (3) + 3 \cdot (-11) = 0
 \end{array}$$

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:

$$11(-c) + 3(4c) = c(-11 + 12) = c(1) = c$$

Another example: Find x and y such that $27x + 15y = 3$. Notice that $\gcd(27,3) = 3$ 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:

$$\begin{array}{llll}
 27 - 1 \cdot 15 = 12 & = \uparrow \leftarrow & = \uparrow \leftarrow & \text{or } 27 \cdot (1) + 15 \cdot (-1) = 12 \\
 15 - 1 \cdot 12 = 3 & = \rightarrow \downarrow \rightarrow & = \downarrow \rightarrow^2 & \text{or } 27 \cdot (-1) + 15 \cdot 2 = 3 \leftarrow \\
 12 - 4 \cdot 3 = 0 & = \uparrow \leftarrow \uparrow^4 \leftarrow^8 & = \uparrow \leftarrow^5 \leftarrow^9 & \text{or } 27 \cdot (5) + 15 \cdot (-9) = 0
 \end{array}$$

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

Another way to find a solution to the equation, $27x + 15y = 3$, is to first divide both sides of the equation by 3 and then solve $9x + 5y = 1$

$$\begin{array}{llll}
 9 - 1 \cdot 5 = 4 & = \uparrow \leftarrow & = \uparrow \leftarrow & \text{or } 9 \cdot (1) + 5 \cdot (-1) = 4 \\
 5 - 1 \cdot 4 = 1 & = \rightarrow \downarrow \rightarrow & = \downarrow \rightarrow^2 & \text{or } 9 \cdot (-1) + 5 \cdot 2 = 1 \leftarrow \\
 4 - 4 \cdot 1 = 0 & = \uparrow \leftarrow \uparrow^4 \leftarrow^8 & = \uparrow \leftarrow^5 \leftarrow^9 & \text{or } 9 \cdot (5) + 5 \cdot (-9) = 0
 \end{array}$$

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

NOTE: The arrows are the same in both methods. Only the value of the arrows change.

What is a solution to the equation $27x + 15y = -3$? $x = \underline{\hspace{1cm}}$, $y = \underline{\hspace{1cm}}$

What is another solution? $x = \underline{\hspace{1cm}}$, $y = \underline{\hspace{1cm}}$

What is a solution to the equation $27x + 15y = 9$? $x = \underline{\quad}$, $y = \underline{\quad}$

What is another solution? $x = \underline{\quad}$, $y = \underline{\quad}$

What is a solution to the equation $27x + 15y = 11$? $x = \underline{\quad}$, $y = \underline{\quad}$

What is another solution? $x = \underline{\quad}$, $y = \underline{\quad}$

What is a solution to the equation $27x + 15y = 0$? $x = \underline{\quad}$, $y = \underline{\quad}$

What is another solution? $x = \underline{\quad}$, $y = \underline{\quad}$

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 combination 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 combination 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 combination 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?

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. $311x-129y=2$

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
						$Q=\text{int}(A/B)$		$R=A-Q*B$		$X2-Q*X1$
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 $B = A*0+B*1$ $V(=X2)$ and $H(=Y2)$ are $X(=X1)$ and $Y(=Y1)$ 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: $A - Q \times B = R$.

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

The program stops.

7 Modular Arithmetic

Modular Arithmetic: Reducing mod m
Rules of Modular Arithmetic

Solving Congruence Equations

Modular Arithmetic: Congruence Equations
Modular Arithmetic: More Congruence Equations
Modular Arithmetic: Common Factors
Modular Arithmetic: Divisibility Rules Explained

Finding Multiplicative Inverses

Modular Arithmetic: Finding Multiplicative Inverses
4-digit Multiplicative Cipher: Mod 10000
4-digit Multiplicative Cipher: Mod 9999
4-digit Multiplicative Cipher: Finding Inverses

Other things
Crickets on Spirals

following

*Multiplicative Ciphers
and Clock Arithmetic*

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

$$m \mid a - b, \text{ read “}m \text{ divides } a - b$$

which is the same as

$$a - b \text{ is a multiple of } m$$

or the same as

$$m \text{ is a factor of } a - b.$$

or the same as

$$a \text{ and } b \text{ have the same remainder when divided by } m$$

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 \equiv used instead of an equal sign, $=$?

Examples: Which statements are true and which are not 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: $a \bmod m$ means the remainder when a is divided by m .

We call the number $a \bmod m$ “ a reduced mod m .” The remainder is always between 0 and $m - 1$, so $a \bmod m$ is always a number between 0 and $m - 1$

Example: The expression “ $37 \bmod 26$ ” means the remainder when dividing 37 by 26. In this case we write $37 \bmod 26 = 11$. Note: It is also true that $37 = 11 \pmod{26}$ and, as well, $11 = 37 \pmod{26}$. It is not true that $11 \bmod 26 = 37$. The right hand side must be a remainder. Explain why each of the following statements is true.

$$53 \bmod 26 = 1$$

$$181 \bmod 8 = 5$$

true: $53 = 2 \cdot 26 + 1$

$$149 \bmod 30 = -1$$

$$173 \bmod 26 = 17$$

false: even though $149 \equiv -1 \pmod{30}$.

Why is the equal sign $=$ used in these last examples instead of symbol \equiv ?

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 not true? Explain your reasoning for each example.

$$-1 \pmod{26} = 25$$

true: $-1 = -1 \cdot 26 + 25$

$$-81 \equiv 807 \pmod{8}$$

$$-18 \equiv 44 \pmod{26}$$

$$-24 \equiv 24 \pmod{26}$$

false: $-24 = 26(-1) + 2$

$$-173 \equiv 121 \pmod{26}$$

$$-77 \equiv 140 \pmod{7}$$

so -24 is equivalent to 2

Rules of Modular Arithmetic

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 $(15 \times 2) + 24 \pmod{26}$

$$\begin{aligned}(15 \times 2) + 24 &\equiv 30 + 24 \pmod{26} & (15 \times 2) + 24 &\equiv 30 + 24 \pmod{26} \\ &\equiv 54 \pmod{26} & &\equiv 4 + 24 \pmod{26} \\ &\equiv 2 \pmod{26} & &\equiv 28 \pmod{26} \\ & & &\equiv 2 \pmod{26}\end{aligned}$$

Example 2: This one is fun:

$$\begin{aligned}23 \times 25 &\equiv 23 \times (-1) \pmod{26} && \text{because } 25 \equiv -1 \pmod{26} !! \\ &\equiv -23 \pmod{26} && \text{because } -23 - 3 = -1 \times 26 \\ &\equiv 3 \pmod{26}\end{aligned}$$

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} .

$$2^{20} = 2^5 \cdot 2^5 \cdot 2^5 \cdot 2^5 \cdot 2^5 = 32^4 \equiv 6^4 \equiv 6^2 \cdot 6^2 \equiv 36 \cdot 36 \equiv 10 \cdot 10 \equiv 100 \equiv 22 \pmod{26}$$

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 $b \pmod{m}$ exactly when $a + c$ is equivalent to $b + c \pmod{m}$.

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?

Modular Arithmetic: Congruence Equations

Like regular arithmetic, the rules on the preceding page are what we need to solve equations in modular arithmetic. Sometimes they are called congruence equations to distinguish them from the type of equations we solve in regular arithmetic.

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: $x \pmod{26} = 3$

$$7 \equiv x - 2 \pmod{12}$$

$$x + 7 \equiv 3 \pmod{13}$$

$$47 \equiv 2 - x \pmod{53}$$

Instead of adding the same number to both sides we 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 $3^{-1} \pmod{26} \equiv 9$. So

$9 \cdot (3x) \equiv 9 \cdot 8 \pmod{26}$	multiplied both sides by 9
$(9 \cdot 3) \cdot x \equiv 9 \cdot 8 \pmod{26}$	applied the associative multiplicative rule
$27 \cdot x \equiv 72 \pmod{26}$	evaluated: $9 \cdot 3 = 27$
$1 \cdot x \equiv 72 \pmod{26}$	reduced: $27 \pmod{26} = 1$
$x \equiv 72 \pmod{26}$	1 is multiplicative identity
$x \equiv 20 \pmod{26}$	reduce: $72 \pmod{26} = 20$

The solution then is any x , such that $x \pmod{26} = 20$.

Solve the following congruence equations. Write your final answer in the form $x \pmod{m} = a$. 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**.

$$2x \equiv 1 \pmod{6}$$

$$2x \equiv 1 \pmod{3}$$

$$2x \equiv 2 \pmod{6}$$

$$3x \equiv 7 \pmod{12}$$

$$3x \equiv 6 \pmod{12}$$

$$6x \equiv 1 \pmod{13}$$

$$4x \equiv 8 \pmod{10}$$

$$5x \equiv 1 \pmod{12}$$

$$5x \equiv 11 \pmod{12}$$

$$7x \equiv 8 \pmod{12}$$

$$8x \equiv 4 \pmod{12}$$

$$29x \equiv 1 \pmod{83}$$

$$29x \equiv 17 \pmod{83}$$

$$91x \equiv 25 \pmod{136}$$

$$132x \equiv 33 \pmod{253}$$

$$132x \equiv 25 \pmod{253}$$

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 two 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 divisibility 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 sum of its 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:

$$10 \pmod{8} = 2$$

$$10^2 \pmod{8} = 2^2 \pmod{8} = 4$$

$$10^3 \pmod{8} = 2^3 \pmod{8} = 0$$

$$10^4 \pmod{8} = 10^3 \cdot 10^1 \pmod{8} = 0$$

$$10^5 \pmod{8} = 10^4 \cdot 10^1 \pmod{8} = 0, \text{ and so on } 10^n \pmod{8} = 0, \text{ for } n > 2.$$

Now consider a number like 4766: $4766 = 4 \cdot 10^3 + 766 \pmod{8} = 0 + 766 \pmod{8}$, 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

$$3x = 1 + 26m \text{ OR}$$

$$3x - 26m = 1 \text{ OR}$$

$$3x + 26y = 1 \text{ (} y=-m \text{)}$$

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 algorithm.

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?

$$\begin{array}{r}
 \square \square \square \square \\
 \times \quad \square 3 \square 7 \\
 \hline
 \square \square \square \square \square \\
 \square \square \square \square \underline{0} \\
 \hline
 \square \underline{0} \underline{0} \underline{0} \underline{1}
 \end{array}$$

(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

$$6600 \times 2973 = 19621800 \equiv 1800 \pmod{10000}$$

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

$$5004 \times 400 = 2001600 = 2000000 + 1600 = 200 \cdot 9999 + 200 + 1600 \equiv 1800 \pmod{9999}$$

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 $10000 \cdot Y + 1$). So we can write an equation:

$$37 \cdot X = 10000 \cdot Y + 1 \quad \text{or} \quad 37 \cdot X - 10000 \cdot Y = 1 \quad \text{or} \quad 37 \cdot X + 10000 \cdot (-Y) = 1$$

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:

$$25 \cdot X = 9999 \cdot Y + 1 \quad \text{or} \quad 25 \cdot X - 9999 \cdot Y = 1 \quad \text{or} \quad 25 \cdot X + 10000 \cdot (-Y) = 1$$

Use the Extended Euclidean Algorithm or find the solution on your calculator.

Procedure: To find the multiplicative inverse of a number, $A \bmod M$, 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.

$$A \cdot X = M \cdot Y + 1 \quad \text{or} \quad A \cdot X - M \cdot Y = 1 \quad \text{or} \quad A \cdot X + M \cdot (-Y) = 1$$

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 MULTIPLICATIVE 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:

$$\begin{array}{r}
 \square \square \square \square \\
 \times \quad \square \square \\
 \hline
 \square \square \square \square \square \\
 \square \square \square \square \square \square \\
 \hline
 \square \square \square \square \square \square \square
 \end{array}$$

$$\begin{array}{r}
 2973 \\
 \underline{\quad 37} \\
 20811 \\
 \underline{89190} \\
 _ 0001
 \end{array}$$

(There may be one more digits to the left in the answer)

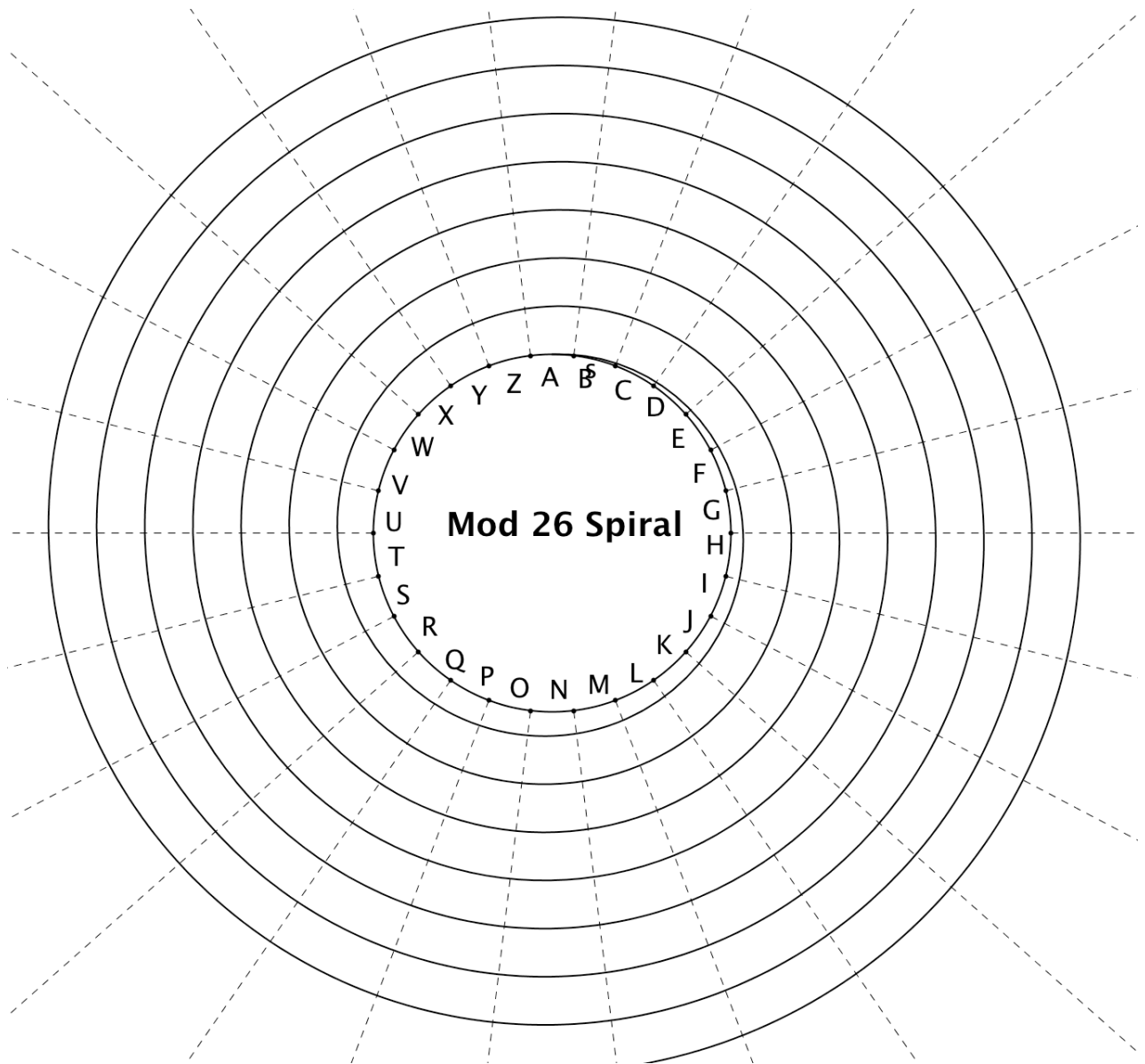
Find the digits that fill in the blanks to make the answer come out as shown.

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.

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?



8 *Prime Numbers*

**Finding Primes without Factoring:
The Sieve of Eratosthenes
Cricket movements on the 200 chart**

**Primes to 10,000 without Factoring
There is an Infinite Number of Prime Numbers
Unique Factorization**

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.

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 is 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
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

Cricket movements on the 200 chart.

These are some cricket moves you might have used on the previous page.

+2: →→ or +10: ↓

+3: →→→ or ↓←

+5: →→→→→ or +10 ↓

+7: →→→→→→→ or ↓←←← or +14: ↓→→→→

+11: ↓→

+13: ↓→→→→ or ↓↓→→→→→→→

Here is a different 200 chart. Now there are 25 numbers in each row.

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	1158	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

Repeat the Sieve of Eratosthenes procedure and notice the difference. Record the cricket moves you use:

+2: →→ or +24: ↓← or +26: ↓→

+3: →→→ or +27 ↓←

+5: →→→→→ or +20 ↓

+7: →→→→→→→ or ↓←←← or +14: ↓→→→→

+11: ↓→

+13: ↓→→→→ or ↓↓→→→→→→→

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, \rightarrow moves once to the right and represents +2. A down arrow, \downarrow 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.

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 $2 \cdot 3 \cdot 5 \cdot 7 \cdot 11 \cdot 13 + 1$ 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,

$$24 = 4 \cdot 6 \text{ and also } 24 = 3 \cdot 8$$

Of course, these numbers can be further factored into prime numbers and in either case if we keep factoring we end up with $2 \cdot 2 \cdot 2 \cdot 3$. 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 .

9 Power Ciphers

Using different mods

Power Ciphers

Finding Patterns in Power Cipher Tables

Power Cipher Mod 37

Fermat's Little Theorem

Power Cipher Mod 55

Power Cipher Mod 437

RSA

Power Ciphers: $n = p \cdot q$

Power Ciphers: RSA Encryption

*following
CME Exponents*

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. Later, we will use very large mods.

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 "p" to get 15. Now compute $15^5 \pmod{26}$. $15^5 \equiv 15^2 \cdot 15^2 \cdot 15 \pmod{26}$ $\equiv 225 \cdot 225 \cdot 15 \pmod{26}$ $\equiv 17 \cdot 17 \cdot 15 \equiv 4335 \pmod{26} \equiv 19$
encode:	15	14	22	04	17	
CIPHERNUMBER:	19	14	16	10	23	

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.

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 power listed for that row. Reduce mod 26.

Example: In row 3, we have

$$1^3 = 1 \pmod{26}, \quad 2^3 = 8 \pmod{26}, \quad 3^3 = 27 \equiv 1 \pmod{26}, \quad 4^3 = 64 \equiv 12 \pmod{26}, \quad \text{etc.}$$

power	Powers mod 26																								
	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
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 repeatedly multiplying by 4, reducing as you go:

$$\begin{aligned} 4^0 &= 1 \equiv 1 \pmod{26} \\ 4^1 &= 4 \cdot 4^0 = 4 \cdot 1 \equiv 4 \pmod{26} \\ 4^2 &= 4 \cdot 4^1 = 4 \cdot 4 \equiv 16 \pmod{26} \\ 4^3 &= 4 \cdot 4^2 = 4 \cdot 16 = 64 \equiv 12 \pmod{26} \\ 4^4 &= 4 \cdot 4^3 = 4 \cdot 12 = 48 \equiv 22 \pmod{26} \\ 4^5 &= 4 \cdot 4^4 = 4 \cdot 22 = 88 \equiv 10 \pmod{26} \\ &\text{etc.} \end{aligned}$$

Compute the other columns in the table. Notice some things about the table:

- In each column, how far before you start repeating?

Depending on the column: 2, 3, 4, 6, 12.

- Which are the good cipher rows?

The good ciphers are rows 1, 5, 7, 11

- How often does the enter row repeat?

Every 12th row

- Which rows, if any, represent the identity cipher?

The 13th, 25th, etc, every twelfth.

- What symmetries do you see in the table?

Notice that it is not symmetric on the diagonal like multiplication and addition. This is because the base and the power do not commute.

- A power cipher has a *power inverse* if you can use a power cipher to decrypt.

- Do the good ciphers have power inverses? If so what are they?

Each good cipher is its own inverse. This will not always be true with other mods. Notice:

$$\begin{aligned} 5 \times 5 &\equiv 1 \pmod{12}, \text{ so } (b^5)^5 = b^{5 \cdot 5} = b^{2 \cdot 12 + 1} = b^{2 \cdot 12} \cdot b^1 = (b^{12})^2 \cdot b^1 \equiv (1)^2 \cdot b = b \\ 7 \times 7 &\equiv 1 \pmod{12} \\ 11 \times 11 &\equiv 1 \pmod{12} \end{aligned}$$

1. With the class, 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?

For prime numbers, the repeating pattern is always a factor of one less than the prime.

- b. Which rows make good ciphers?

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 $0 \pmod{m}$.

- c. Find power inverses whenever possible.

For prime mods, any number is a good key for a power cipher.

Power Cipher Mod 37

First, we'll make an alphabet that has 37 letters. We add the period (.) To the letters and single digit numerals. 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 with 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

$$a^{37} = a \pmod{37} \text{ for all } a. \quad (\text{fact 1})$$

(this, by the way, makes 37 a “good” key because the inverse of the identity is the identity)

$$a^{36} = 1 \pmod{37} \text{ for all } a. \quad (\text{fact 2})$$

(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, n . Then raising to the n th power followed by raising to the m th 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 good power keys mod 37 are just those numbers, n , that are relatively prime to 36.

Examples: Decrypt this message, that was encrypted using a power cipher mod 37 with key = 7. [HINT: $7 \cdot 31 = 217 = 6 \cdot 36 + 1$]

t h e k e y i s 7
29 17 14 20 14 34 18 28 07

1. Pick another good power cipher key mod 37 and encrypt your name.

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 those numbers that are relatively prime to $p-1$

Power Cipher Mod 55

As observed in the power table mod 55, the good ciphers mod 55 are those powers that are relatively prime to 40. Notice that $55 = 5 \cdot 11$ and $(5-1) \cdot (11-1) = 4 \cdot 10 = 40$.

The good ciphers are

1, 3, 7, 9, 11, 13, 17, 19, 21, 23, 27, 29, 31, 33, 37, 39

Encrypt something using the power cipher 13:

Decrypt this word that was encrypted using the power cipher 19

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 do not want to decode back to letters.

Even having the table, it may be easier to do computations.

Power Cipher Mod 437

Because $437 = 23 \cdot 19$ the good power ciphers mod 437 are those powers that are relatively prime to $(23-1) \cdot (19-1) = 22 \cdot 18 = 396$.

List 5 numbers that are relatively prime to 396

Any prime number that is not a divisor of 396 is relatively prime to 396, for example: 47. The inverse of 17 mod 396 is 59.

[Confirm that $47 \cdot 59 = 2773 = 7 \cdot 396 + 1$]

Find the inverses mod 396 of the numbers you listed in 1.

Example: Use the power cipher 47 to encrypt the letters:

P	O	W	E	R
15	14	22	04	17
155	260	390	225	175

Example: Check the work by raising each cipher number to the 59th power:

$155^{59} \equiv 15 \pmod{437}$
 $260^{59} \equiv 14 \pmod{437}$
 $390^{59} \equiv 22 \pmod{437}$
 $225^{59} \equiv 4 \pmod{437}$
 $175^{59} \equiv 17 \pmod{437}$

Make our own power cipher mod 437. Make sure you know how to encrypt and decrypt. Encrypt a four letter secret password.

Power Ciphers: $n = p \cdot q$

In this project you will make your own power cipher from scratch. You will choose your modulus that is the power of two primes: $n = p \cdot q$. You will choose a number, e , that is relatively prime to $(p-1) \cdot (q-1)$. You will find the inverse of $e \pmod{(p-1) \cdot (q-1)}$.

Pick two prime numbers. Both should be larger than 50. Call them p and q .

$$p = \underline{\hspace{2cm}}$$

$$q = \underline{\hspace{2cm}}$$

$$n = p \cdot q = \underline{\hspace{2cm}}$$

$$(p-1) \cdot (q-1) = \underline{\hspace{2cm}}$$

Find a number, call it e , that is relatively prime to $(p-1) \cdot (q-1)$.

$$e = \underline{\hspace{2cm}}$$

Find $e^{-1} \pmod{(p-1) \cdot (q-1)}$.

$$e^{-1} = \underline{\hspace{2cm}}$$

2. To check your work, do the following

Compute 4^e . Answer = _____

Take the Answer and raise it to the power e^{-1} . Answer = _____

3. Think of a good four-letter password. Encrypt it with your power cipher. Check your work raising each number in your encryption to the 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, using 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 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 .

$$p = \underline{\hspace{2cm}}$$

$$q = \underline{\hspace{2cm}}$$

$$n = p \cdot q = \underline{\hspace{2cm}}$$

$$(p-1) \cdot (q-1) = \underline{\hspace{2cm}}$$

Find a number, call it e , that is relatively prime to $(p-1) \cdot (q-1)$.

$$e = \underline{\hspace{2cm}}$$

(n, e) is called your *public key*.

Find $e^{-1} \pmod{(p-1) \cdot (q-1)}$.

$$e^{-1} = \underline{\hspace{2cm}}$$

e^{-1} is your private key

1. To check your work, do the following

Compute 4^e . Answer = _____

Take the Answer and raise it to the power e^{-1} . Answer = _____

2. Put your private key into the class directory of public keys. Remember your private key but don't tell it to anyone.