What is the clumsiest bee?

B C V N C M J O H C F F

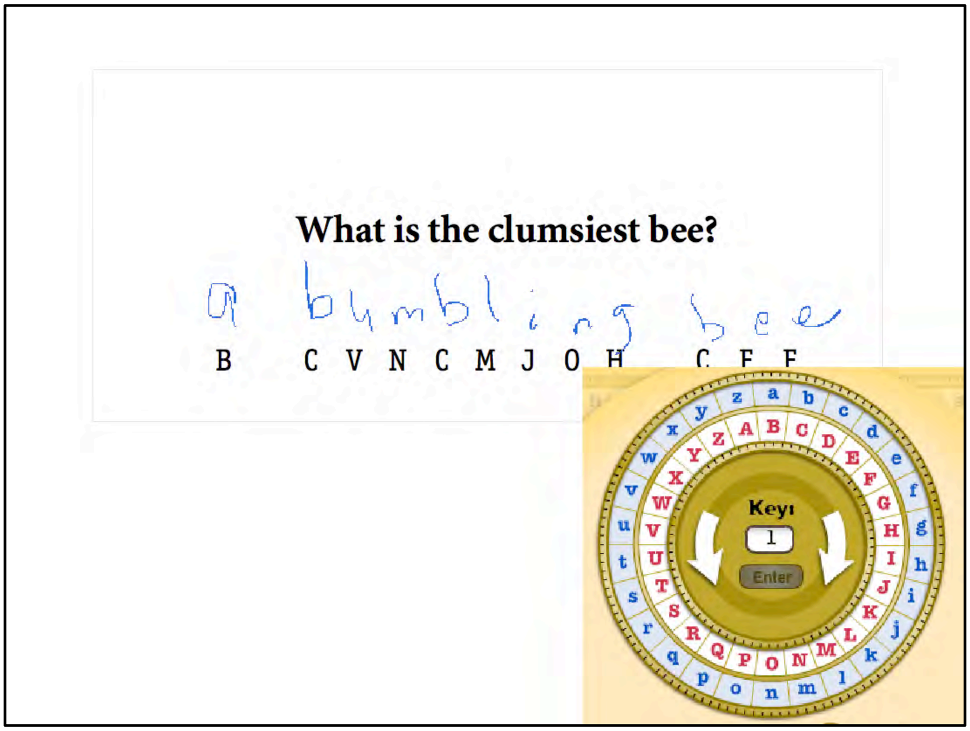
No experience in Cryptography can get started until everyone has had a chance to crack a message and solve a riddle.

What is the clumsiest bee?

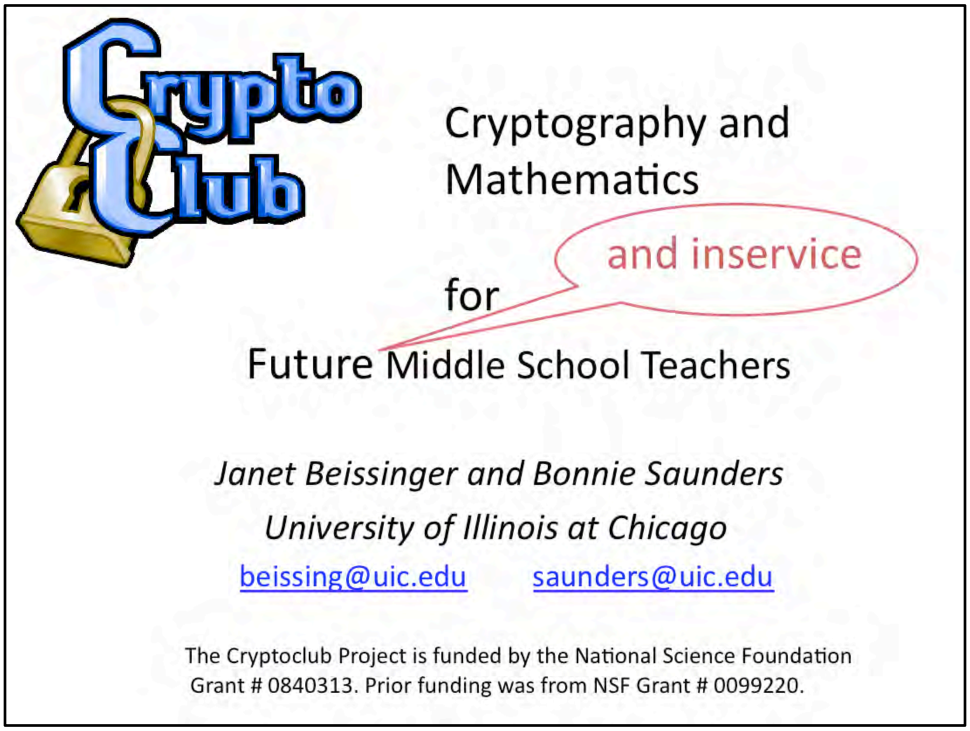
a bumbling bee

B C V N C M J O H C F F

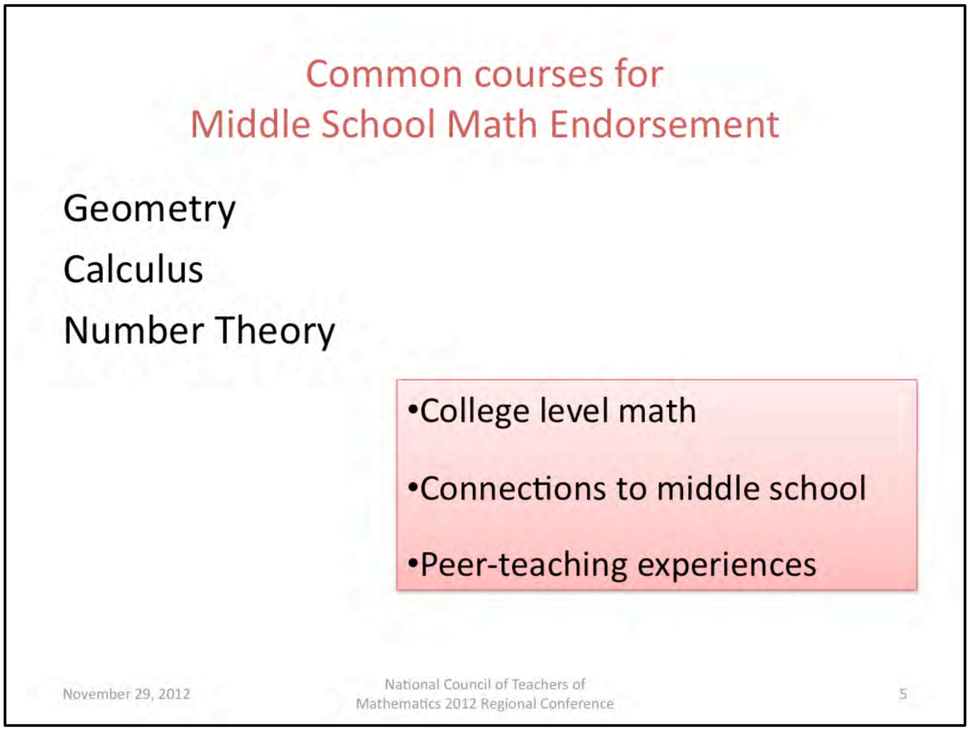
Every student can start off with successl. They crack the message AND
they see a pattern: every plaintext letter is just one before (in the alphabet) the ciphertext letter.



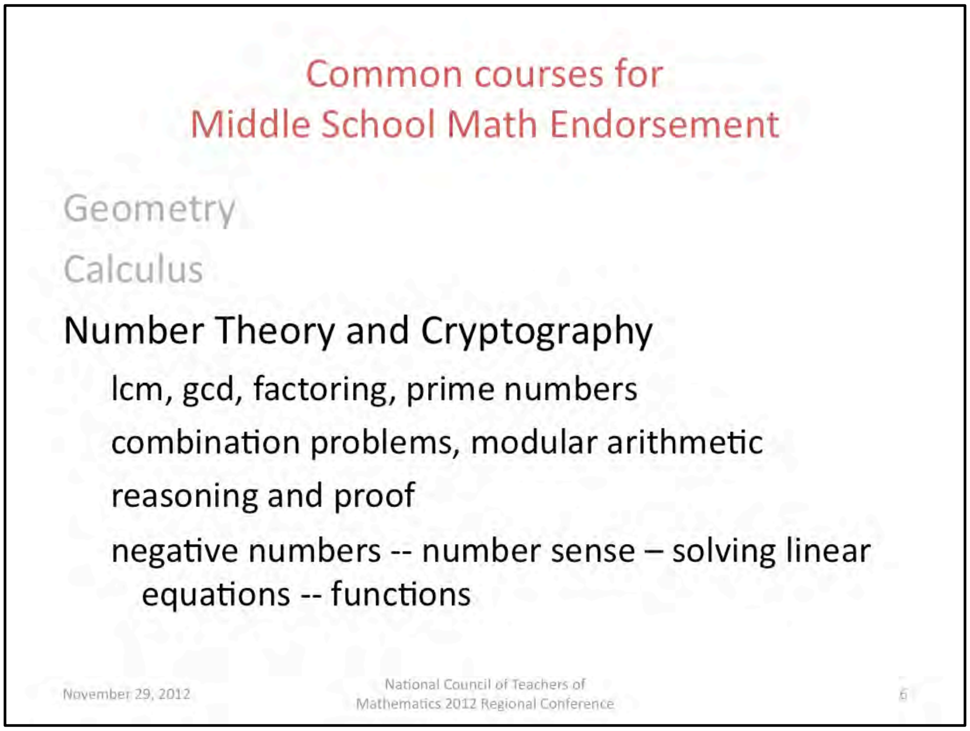
A Cipher Wheel is a tool that allowsthe cryptographer to ecnrypt/decrypt any shift of the alphabet. This wheel is set to encrypt/decrypt a shift of 1.



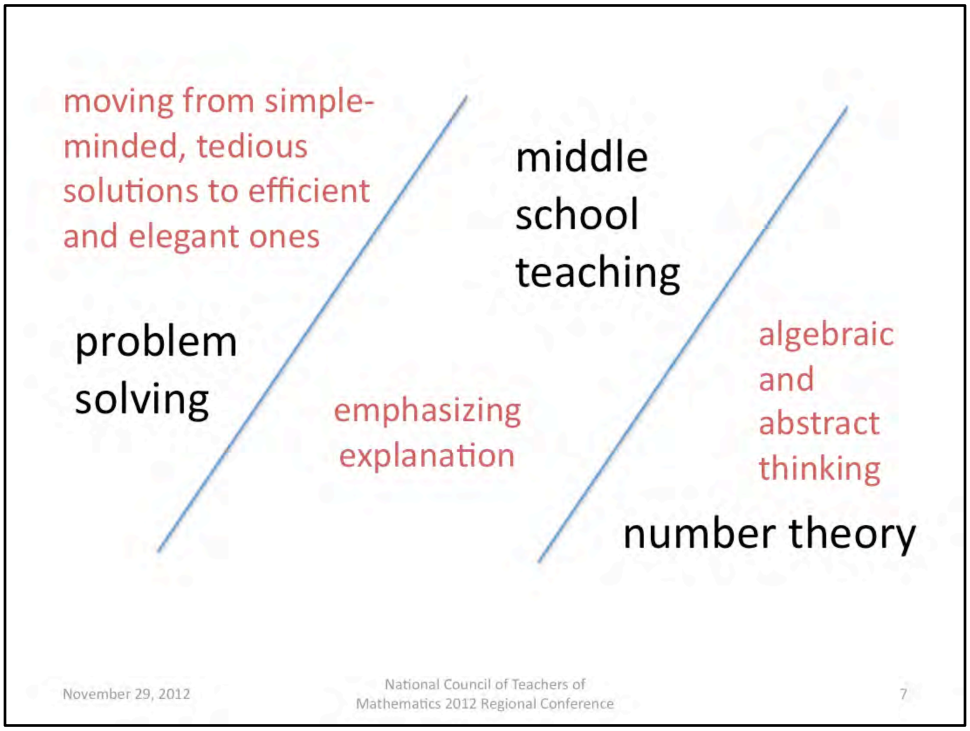
CryptClub is an nsf funded project to develop hands-on and online materials for use in afterschool (and other informal learning) programs. Materials from this project appear throughout the talk. But the talk itself is about a course for preservice teachers (also modified for inservice teachers).



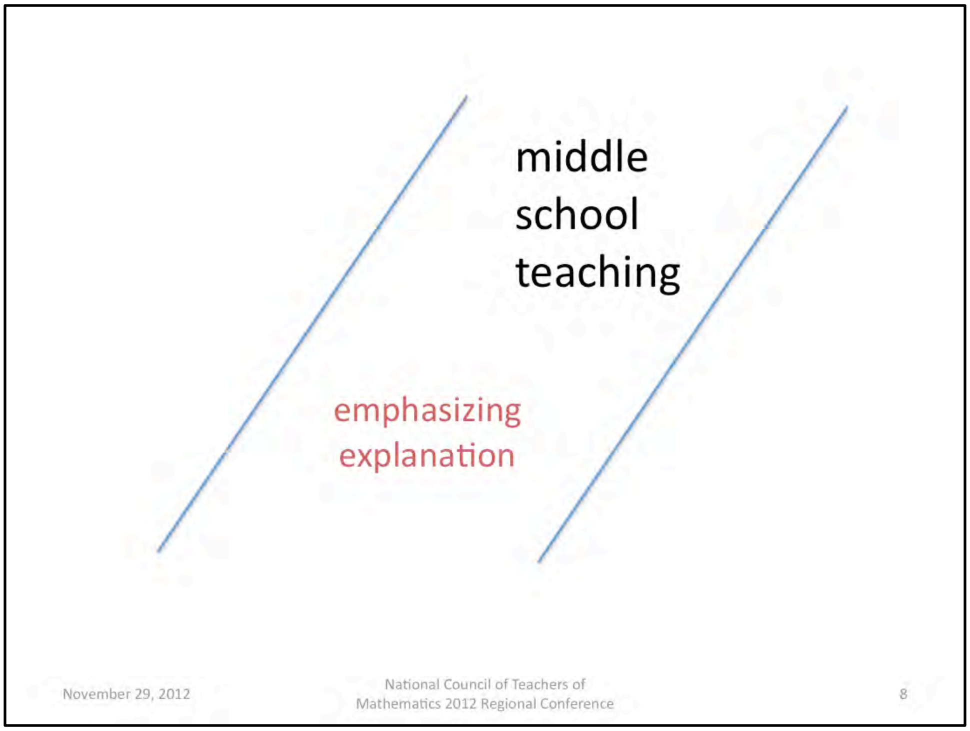
At UIC the math department offers a mathematics concentration to elementary education majors. When they finish their degree with the College of Education they will receive, besides teacher certification, the middle school math endorsement. There are three core courses for these students. The philosophy of the department is that they should
1) learn some piece of more advances mathematics. 2) be be reminded of middle school math topics connected to the subject of the course, and 3) have experience teaching the newly learned material to each other.



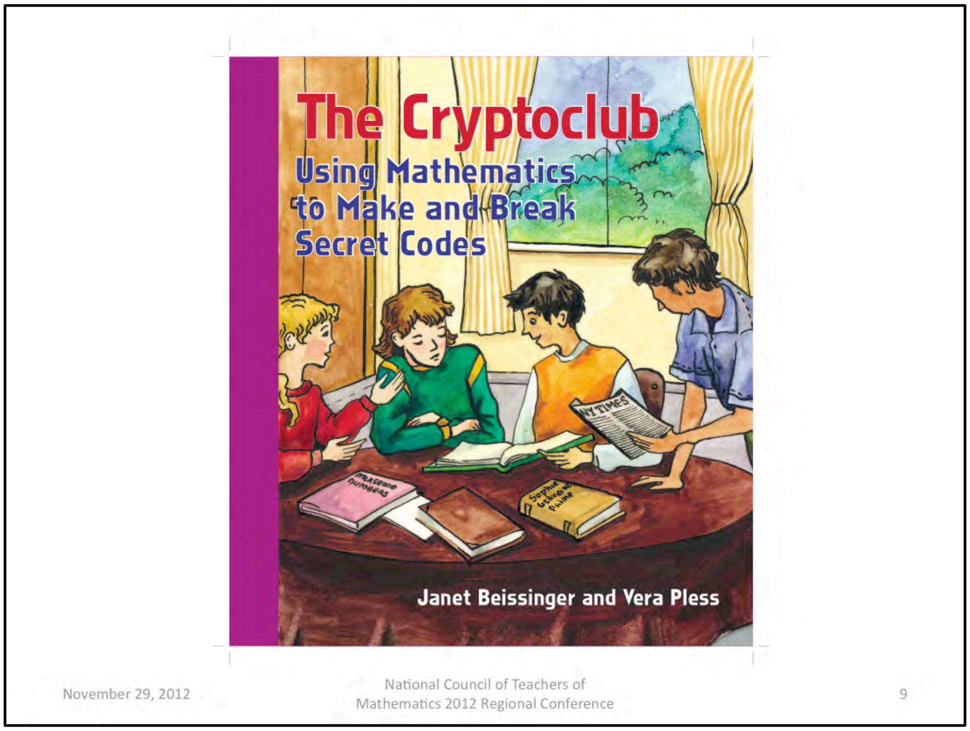
Some of the topics covered in CryptoClub and/or in this cryptography course. Number Theory does not appear as a subject itself in existing standards (It was a standard on its own in the original NCTM Standards – 1989). For better or worse, it is often delegated to the problem solving, reasoning strands, such as the mathematical practices of CCSSM



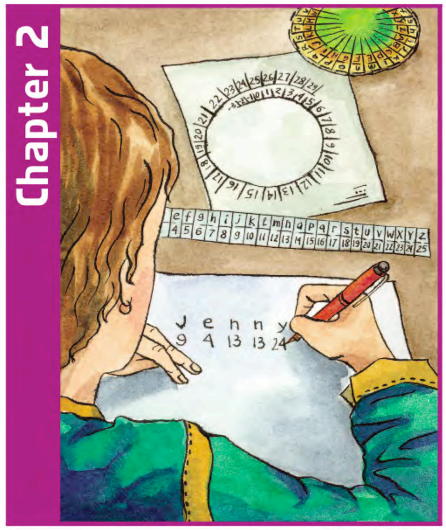
Learning to explain your solution precisely can lead to the more elegant solution strategies– including algebraic. The process is one of developing communication skills and moving to more abstract thinking. I hope to show by a few examples the connections between these components.



Examples of “teaching” done by students in the course are not included in this document.



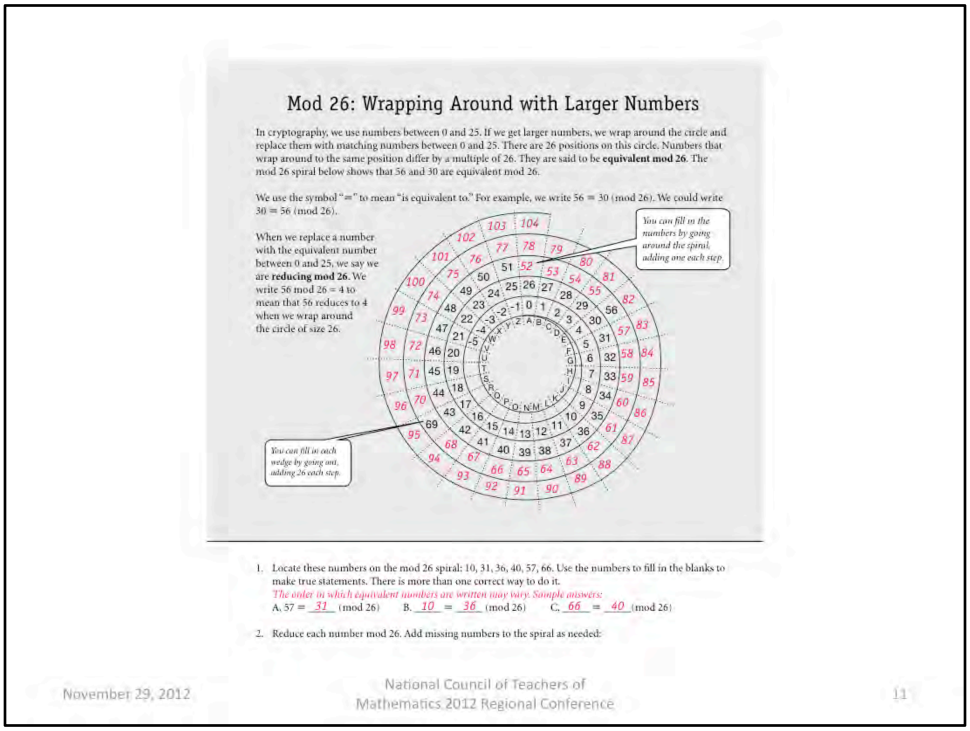
This book contains lots of examples of lessons that preservice teachers can “teach” each other. The book includes great explanations, practice problems, messages to encrypt, decrypt and crack, and other application of number theory problems.



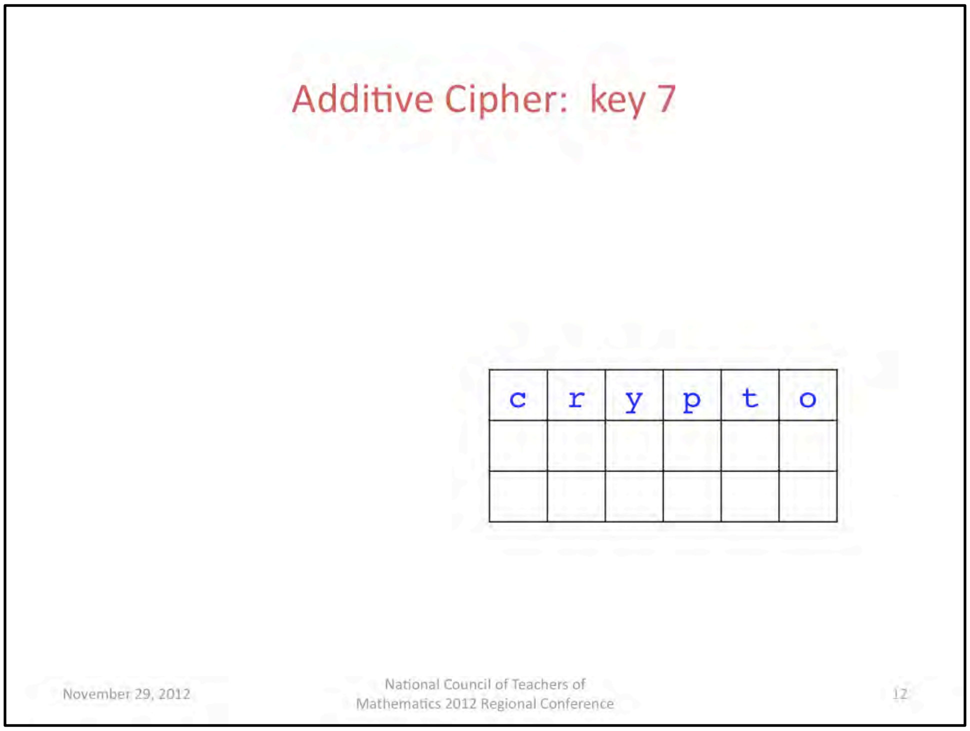
8 Unit 1: Introduction to Cryptography

November 29, 2012 National Council of Teachers of Mathematics 2012 Regional Conference 10

To use mathematics, we are going to have to think about letters as numbers. We assign a number 0 to 25 to each letter as shown here.



However, once we get going, we will get larger and larger numbers so we need a way of converting all numbers to letters. SO we use this spiral that wraps the number around the circle of letters – 26 numbers in each wrap. Kids love this spiral but the goal is to be able to find what letter for a given number, without the spiral, or for the very large numbers that don't appear. Finding strategies to do this is a great activity for middle school kids and teachers. This ultimately involves understanding division with remainder – a number is wrapped around in multiples of 26 and the remainder shows the exact location on the wheel.



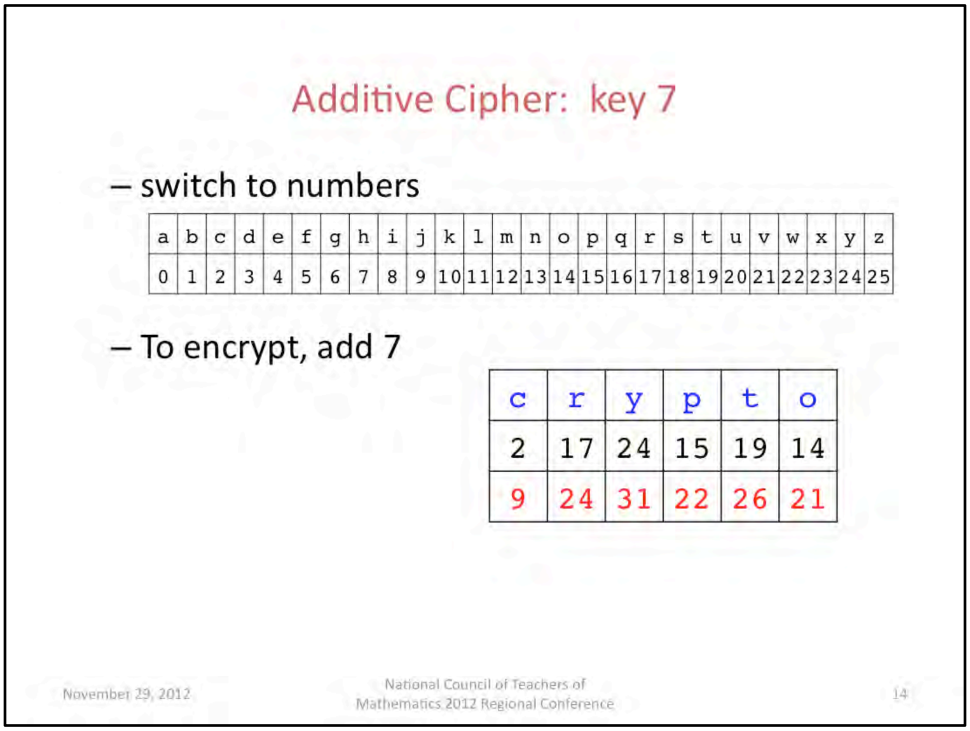
Next let's look in more detail at the first cipher in the book that uses numbers: the additive cipher.

Additive Cipher: key 7

– switch to numbers

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

c	r	y	p	t	o
2	17	24	15	19	14



Subtract 26 to reduce 31 to 5 and 26 to 0. Using the Mod 26 Spiral is another way to reduce. With later numbers, reducing involves finding the remainder when dividing by 26.

Additive Cipher: key 7

– switch to numbers

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

– To encrypt, add 7

– Reduce mod 26

c	r	y	p	t	o
2	17	24	15	19	14
9	24	5	22	0	21

Additive Cipher: key 7

9	18	1	8

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

Additive Cipher: key 7

– To decrypt, subtract 7

9	18	1	8

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

show wheel
additive inverse –abstract part
-- show video
show multiplication table

Additive Cipher: key 7

– To decrypt, subtract 7

2	11	-6	1
9	18	1	8

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

Additive Cipher: key 7

– To decrypt, subtract 7

– Reduce mod 26

2	11	20	1
9	18	1	8

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

show wheel
additive inverse –abstract part
-- show video
show multiplication table

Additive Cipher: key 7

- To decrypt, subtract 7
- Reduce mod 26
- Switch to letters

c	l	u	b
2	11	20	1
9	18	1	8

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

Additive Cipher: key 7

– To decrypt, add 26 – 7 = 19

2	11		1
9	18	1	8

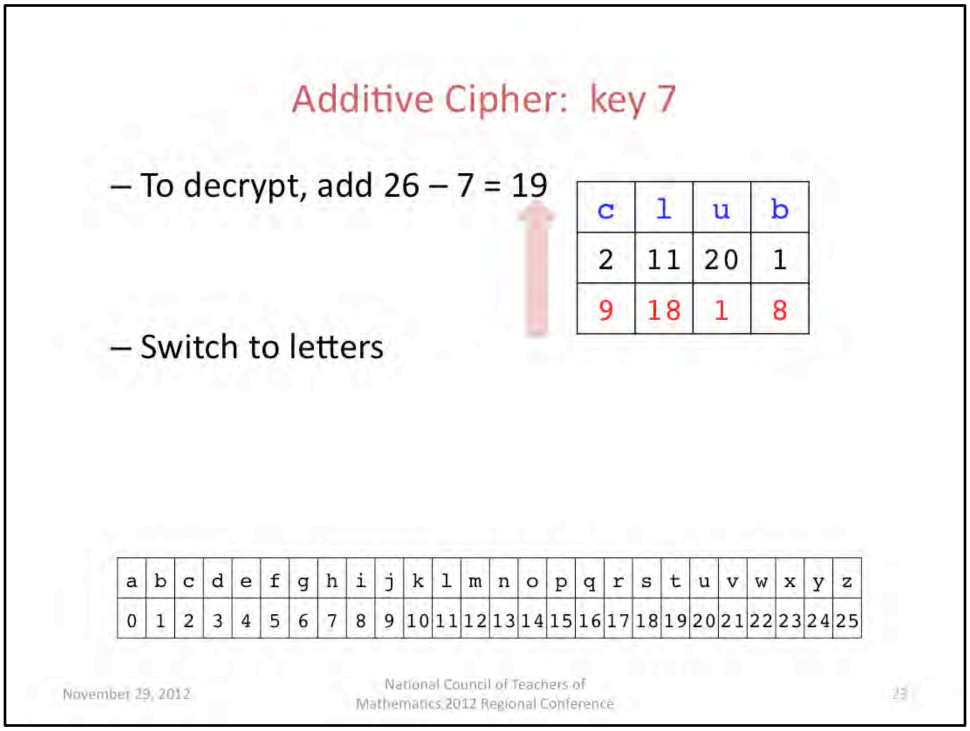
a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z
0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25

Additive Cipher: key 7

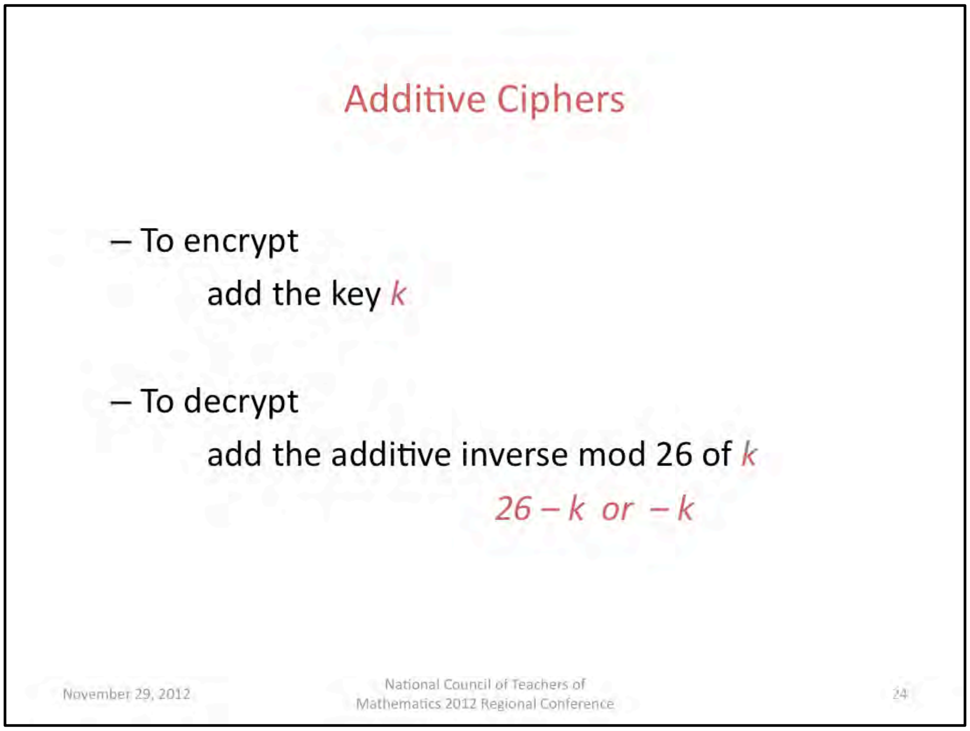
– To decrypt, add 26 – 7 = 19

2	11	20	1
9	18	1	8

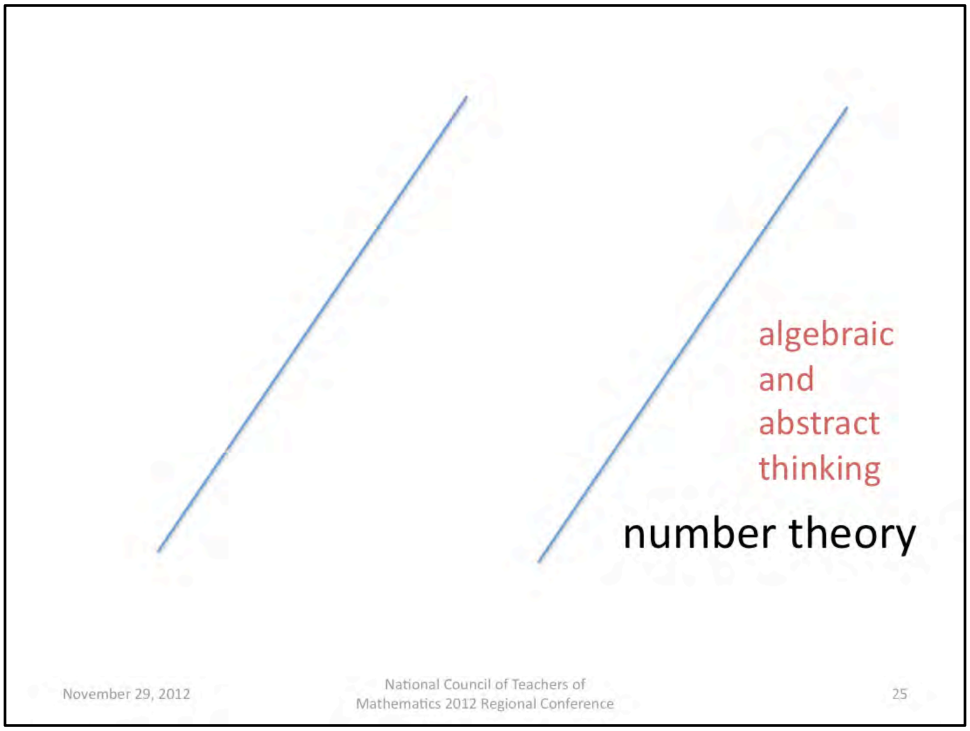
a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z
0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25



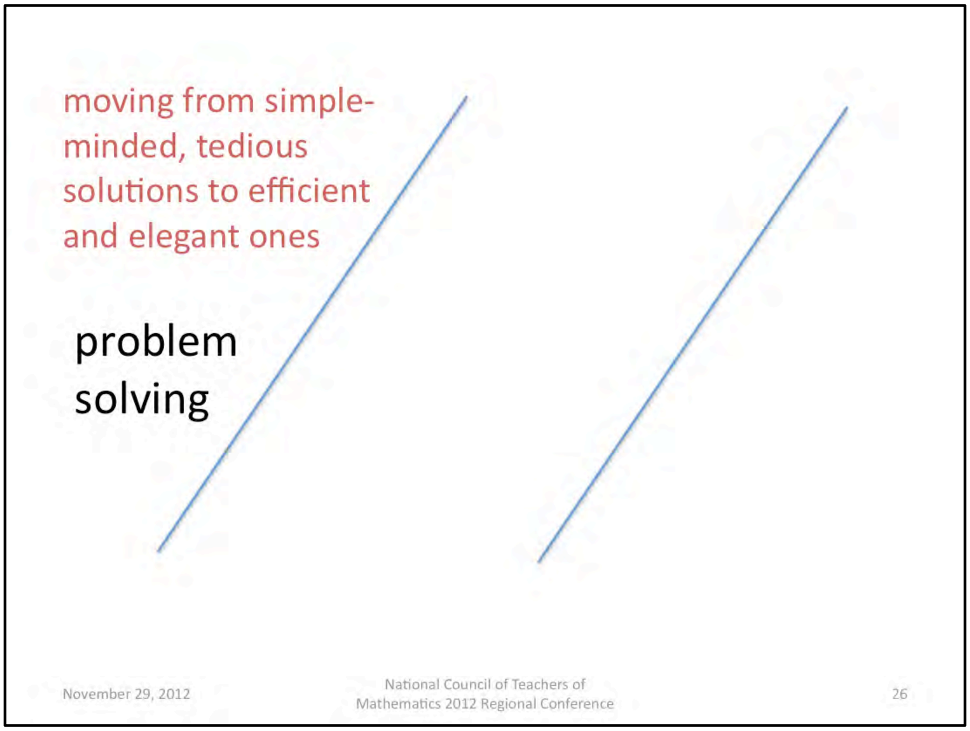
show wheel
additive inverse –abstract part
-- show video
show multiplication table



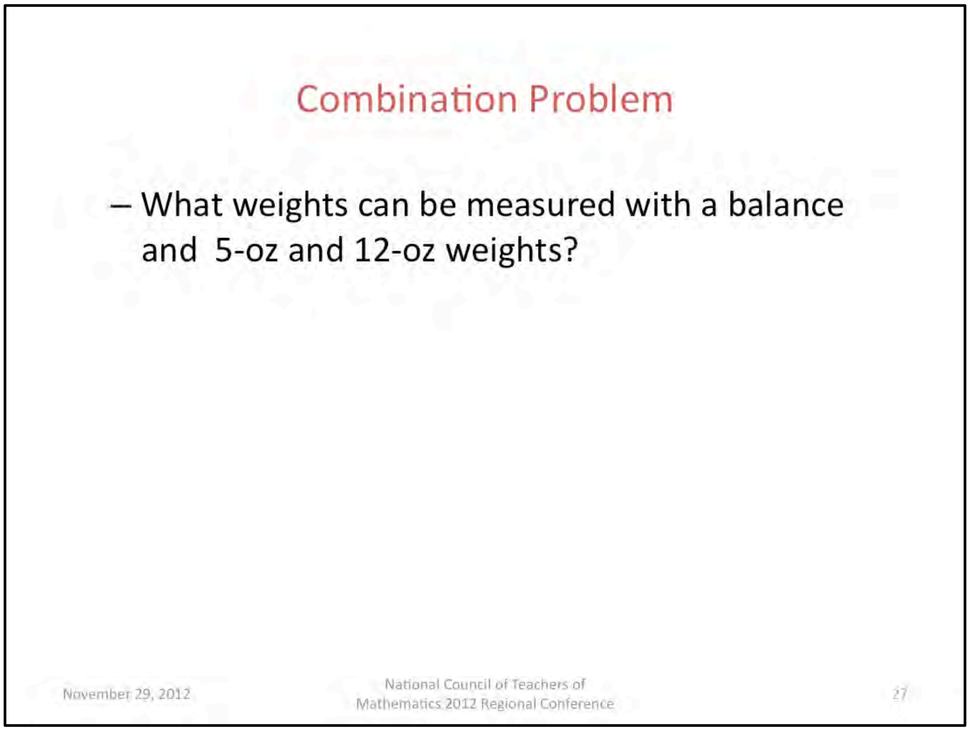
This is now a more abstract view point. Note that, among other things decryption can now be viewed as the same thing as encryption. The inverse process is the same – just using an "inverse" key.



The idea of inverse is an example of abstract thinking, thinking more deeply about the structure of number systems.



Problems Solving Project – I have a growing list of problems inspired by number theoretic concerns that are
doable by elementary and/or middle school students – either with or without learning
the supporting, possibly more abstract, mathematics.



One example to consider: a combination problem.
Looking at Combinations from the *Mathematics in Context* MS Curriculum

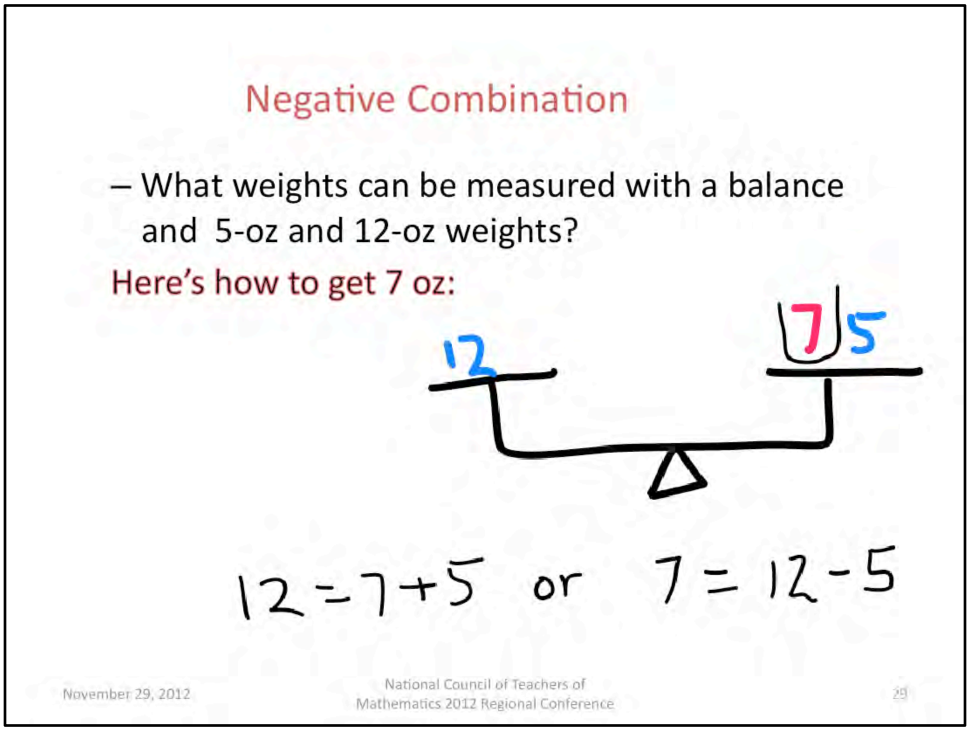
Combination Chart

Number of 12-oz weights

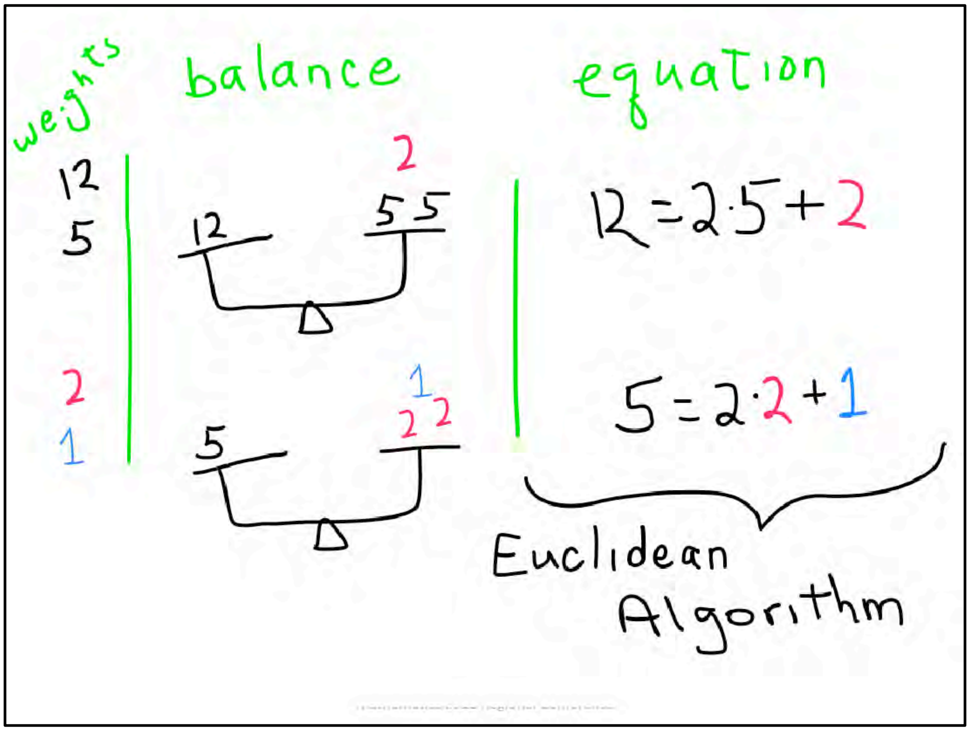
12	144	149	154	159	164	169	174	179	184	189	194	199	204	209	214	219
11	132	137	142	147	152	157	162	167	172	177	182	187	192	197	202	207
10	120	125	130	135	140	145	150	155	160	165	170	175	180	185	190	195
9	108	113	118	123	128	133	138	143	148	153	158	163	168	173	178	183
8	96	101	106	111	116	121	126	131	136	141	146	151	156	161	166	171
7	84	89	94	99	104	109	114	119	124	129	134	139	144	149	154	159
6	72	77	82	87	92	97	102	107	112	117	122	127	132	137	142	147
5	60	65	70	75	80	85	90	95	100	105	110	115	120	125	130	135
4	48	53	58	63	68	73	78	83	88	93	98	103	108	113	118	123
3	36	41	46	51	56	61	66	71	76	81	86	91	96	101	106	111
2	24	29	34	39	44	49	54	59	64	69	74	79	84	89	94	99
1	12	17	22	27	32	37	42	47	52	57	62	67	72	77	82	87
0	0	5	10	15	20	25	30	35	40	45	50	55	60	65	70	75
	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15

Number of 5-oz weights

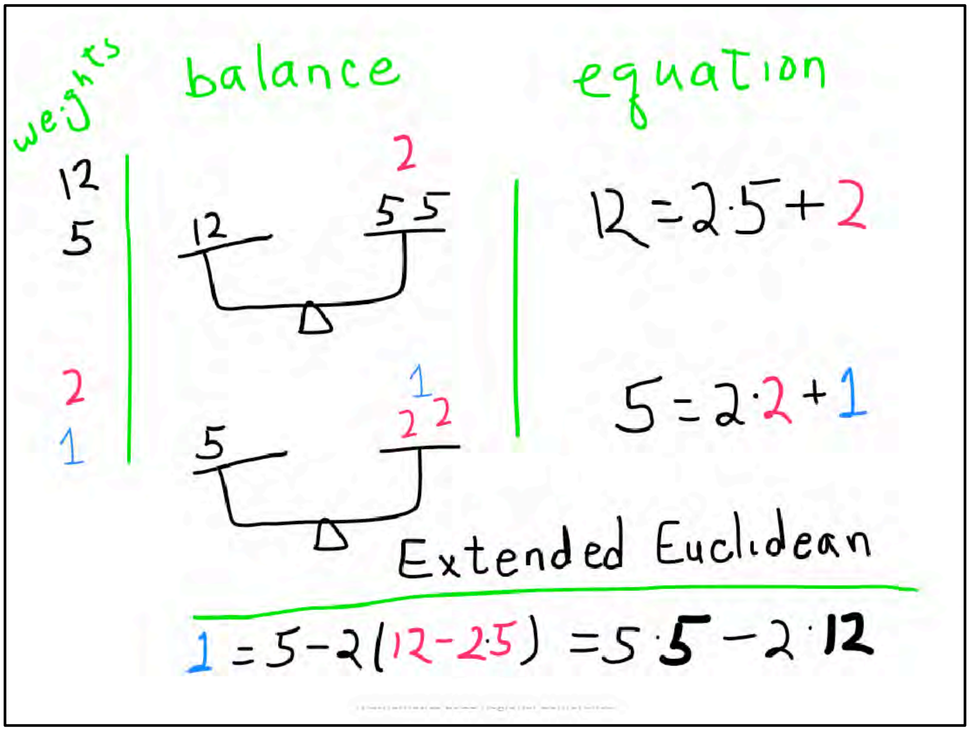
This chart shows all combinations of 12 and 5. Generally, people find it fun to solve this problem by their own wits, but a table like this is good for understanding the problem – and a tool we use extensively in the course. But there are some weights that are missing. For example 43. Can I realize theses missing weights? The answer is yes. To see why we start with an easier example: 7



7 is a "negative combination of 12 and 5



Here's how to get a 1 oz weight. The equations show the Euclidean Algorithm For other numbers the algorithm ends with the greatest common divisor of the two starting weights. Both preservice and inservice teachers tend to like this algorithm – it is a fun procedure for them and it's a way to find the gcd of two numbers without factoring.



One can “unwind” the equations to find the combination of 12 and 5 that gives 1. This process can be accomplished by keeping track of combinations throughout the steps in the Euclidean Algorithm. That process is called the Extended Euclidean Algorithm.

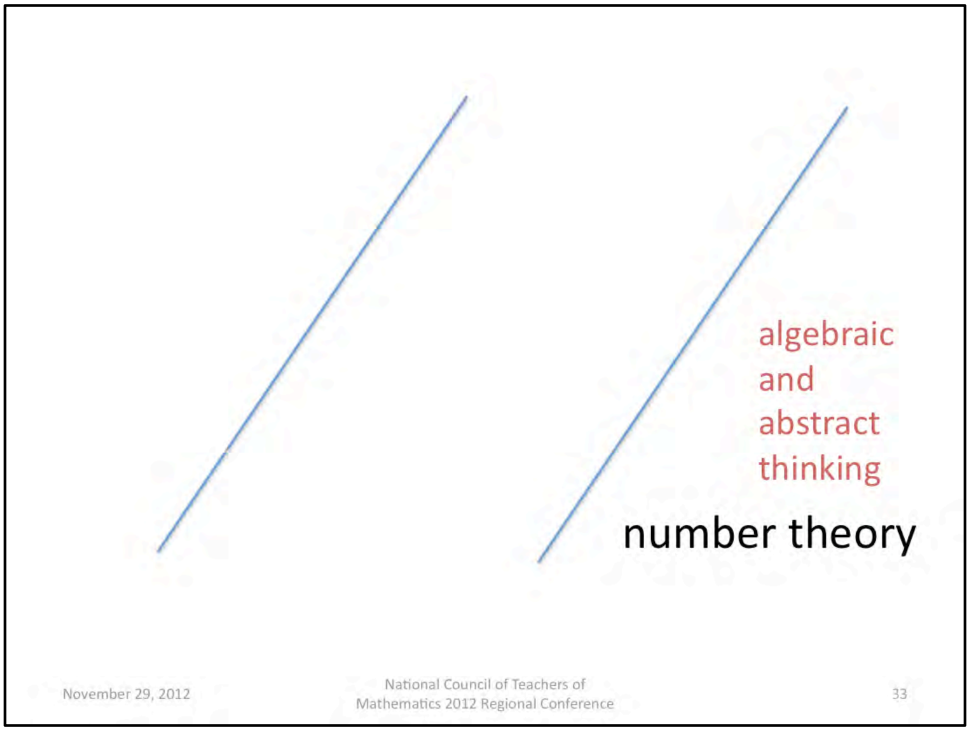
Combination Chart

Number of 12-oz weights

9	83	88	93	98	103	108	113	118	123	128	133	138	143	148	153	158
8	71	76	81	86	91	96	101	106	111	116	121	126	131	136	141	146
7	59	64	69	74	79	84	89	94	99	104	109	114	119	124	129	134
6	47	52	57	62	67	72	77	82	87	92	97	102	107	112	117	122
5	35	40	45	50	55	60	65	70	75	80	85	90	95	100	105	110
4	23	28	33	38	43	48	53	58	63	68	73	78	83	88	93	98
3	11	16	21	26	31	36	41	46	51	56	61	66	71	76	81	86
2	-1	4	9	14	19	24	29	34	39	44	49	54	59	64	69	74
1	-13	-8	-3	2	7	12	17	22	27	32	37	42	47	52	57	62
0	-25	-20	-15	-10	-5	0	5	10	15	20	25	30	35	40	45	50
-1	-37	-32	-27	-22	-17	-12	-7	-2	3	8	13	18	23	28	33	38
-2	-49	-44	-39	-34	-29	-24	-19	-14	-9	-4	1	6	11	16	21	26
-3	-61	-56	-51	-46	-41	-36	-31	-26	-21	-16	-11	-6	-1	4	9	14
	-5	-4	-3	-2	-1	0	1	2	3	4	5	6	7	8	9	10

Number of 5-oz weights

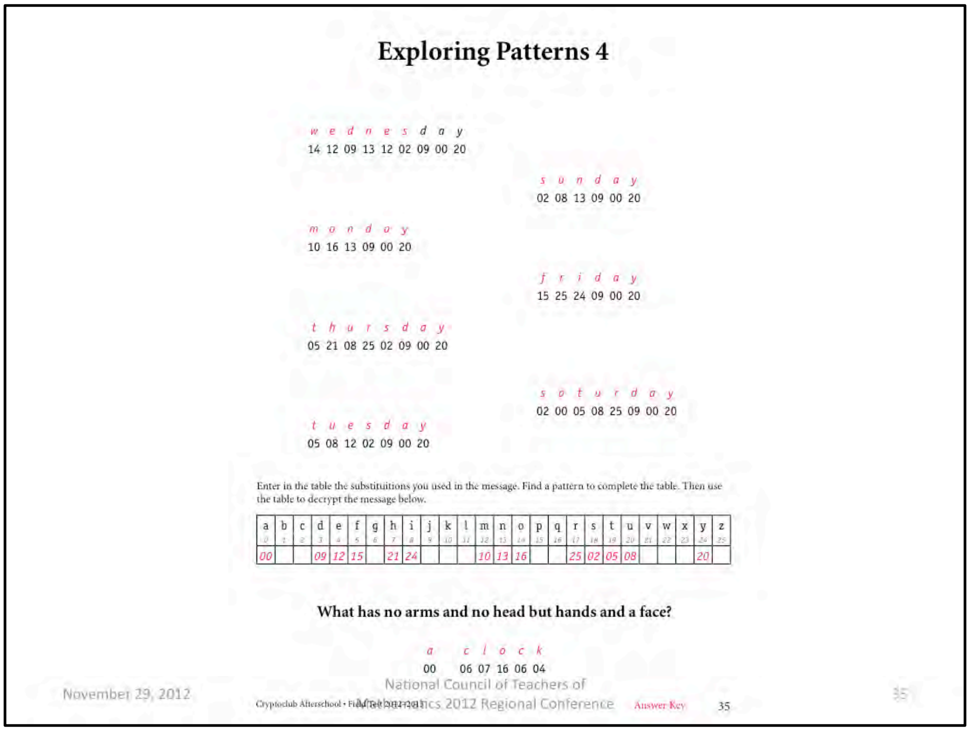
This chart shows some of the negative combinations. Every integer will appears on the chart (if the chart is extended properly.



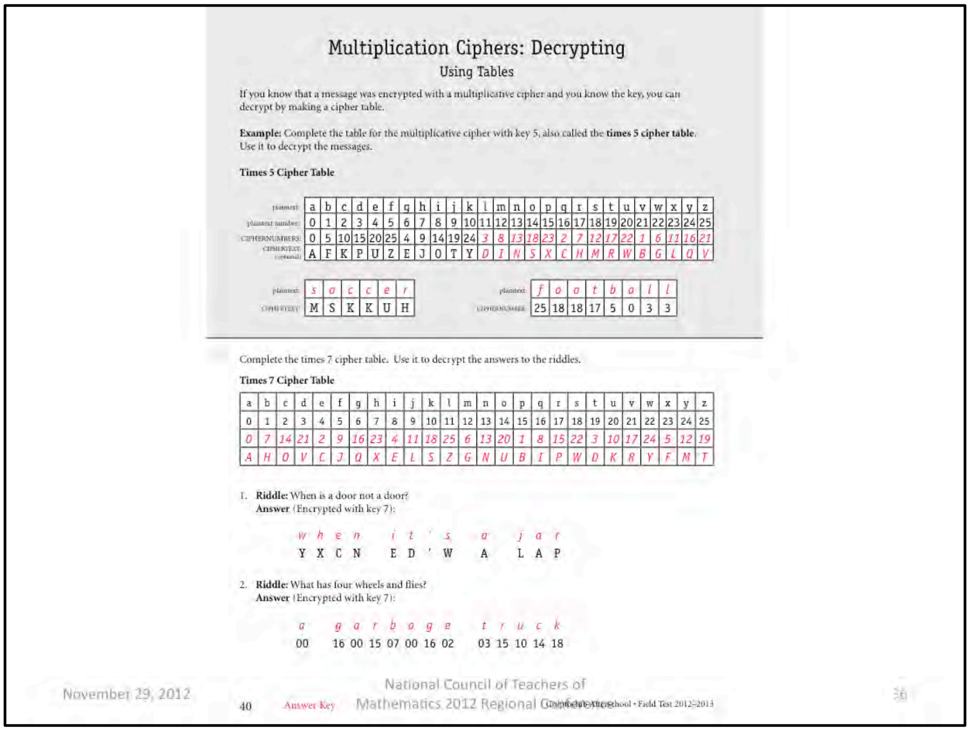
Learning the Euclidean Algorithm and the Extended Euclidean Algorithm give (future) teachers a chance to explore more advanced mathematics that has a strong connected to middle school mathematics. They may never present it to students but they have a much deeper understanding of the topic.

What does that have to do with Cryptography?

What does this have to do with Cryptography: To see what this has to do with Cryptography, the next few slides present a quick introduction to the Multiplicative Cipher.



We always begin a new cipher with cracking a cipher and looking for patterns. Student will discover the multiplicative pattern in the cipher table.



Multiplication Ciphers: Decrypting

Using Tables

If you know that a message was encrypted with a multiplicative cipher and you know the key, you can decrypt by making a cipher table.

Example: Complete the table for the multiplicative cipher with key 5, also called the **times 5 cipher table**. Use it to decrypt the messages.

Times 5 Cipher Table

plaintext:	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
plaintext number:	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25
CIPHERNUMBERS:	0	5	10	15	20	25	4	9	14	19	24	3	8	13	18	23	2	7	12	17	22	1	6	11	16	21
CIPHERTEXT: (optional)	A	F	K	P	U	Z	E	J	O	T	Y	D	I	N	S	X	C	H	M	R	W	B	G	L	Q	V

plaintext:	s	o	c	c	e	r
CIPHERTEXT:	M	S	K	K	U	H

plaintext:	f	o	o	t	b	a	l	l
CIPHERNUMBER:	25	18	18	17	5	0	3	3

Complete the times 7 cipher table. Use it to decrypt the answers to the riddles.

Times 7 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
0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25
0	7	14	21	2	9	16	23	4	11	18	25	6	13	20	1	8	15	22	3	10	17	24	5	12	19
A	H	O	V	C	J	Q	X	E	L	S	Z	G	N	U	B	I	P	W	D	K	R	Y	F	M	T

1. **Riddle:** When is a door not a door?
   Answer (Encrypted with key 7):

   w h e n   i t ' s   a   j a r
   Y X C N   E D ' W   A   L A P

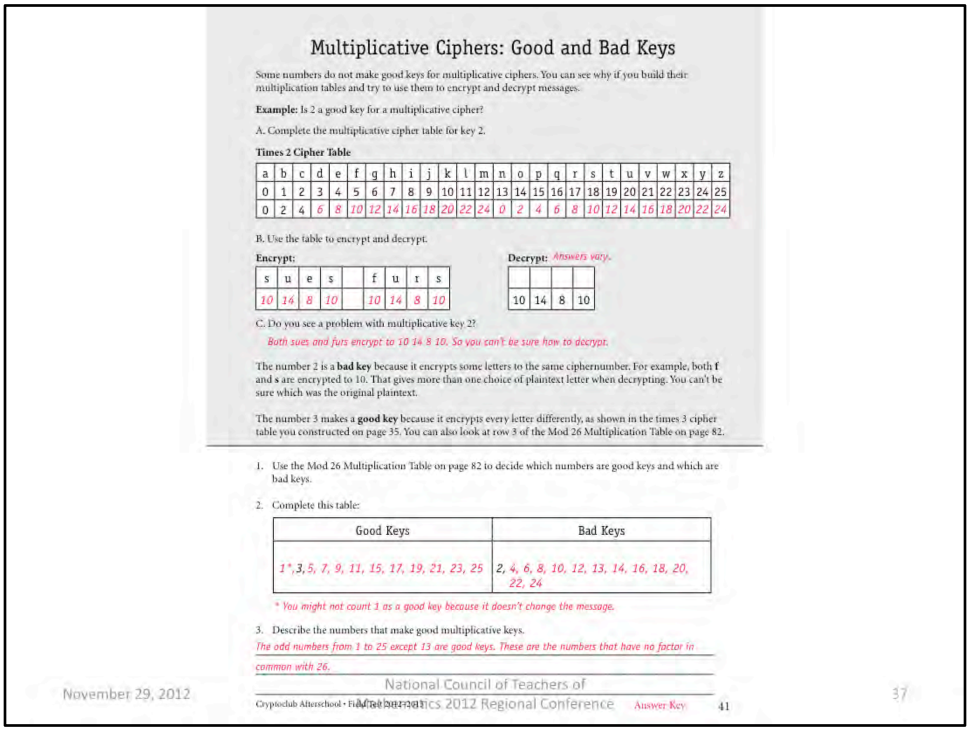
2. **Riddle:** What has four wheels and flies?
   Answer (Encrypted with key 7):

   a   g a r b a g e   t r u c k
   00   16 00 15 07 00 16 02   03 15 10 14 18

40 Answer Key Middle School • Field Test 2012–2013

November 29, 2012 National Council of Teachers of Mathematics 2012 Regional Conference 36

Then they can make multiplicative cipher tables using other keys.



Multiplicative Ciphers: Good and Bad Keys

Some numbers do not make good keys for multiplicative ciphers. You can see why if you build their multiplication tables and try to use them to encrypt and decrypt messages.

Example: Is 2 a good key for a multiplicative cipher?

A. Complete the multiplicative cipher table for key 2.

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

B. Use the table to encrypt and decrypt.

Encrypt:

s	u	e	s		f	u	r	s
10	14	8	10		10	14	8	10

Decrypt: *Answers vary.*

10	14	8	10

C. Do you see a problem with multiplicative key 2?

Both sues and furs encrypt to 10 14 8 10. So you can't be sure how to decrypt.

The number 2 is a **bad key** because it encrypts some letters to the same ciphernumber. For example, both **f** and **s** are encrypted to 10. That gives more than one choice of plaintext letter when decrypting. You can't be sure which was the original plaintext.

The number 3 makes a **good key** because it encrypts every letter differently, as shown in the times 3 cipher table you constructed on page 35. You can also look at row 3 of the Mod 26 Multiplication Table on page 82.

1. Use the Mod 26 Multiplication Table on page 82 to decide which numbers are good keys and which are bad keys.
2. Complete this table:

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

* *You might not count 1 as a good key because it doesn't change the message.*

3. Describe the numbers that make good multiplicative keys.

The odd numbers from 1 to 25 except 13 are good keys. These are the numbers that have no factor in common with 26.

But problems arise. When calculating the times 2 cipher, things go well until you get to 13. 2 times 13 is 0 (mod 26) but 2 times 0 is also 0. This is a BAD cipher. It is not a 1-1 function: more than one letter is assigned to the same number. Students will discover that the BAD keys are those that have common factors with 26.

key = 14

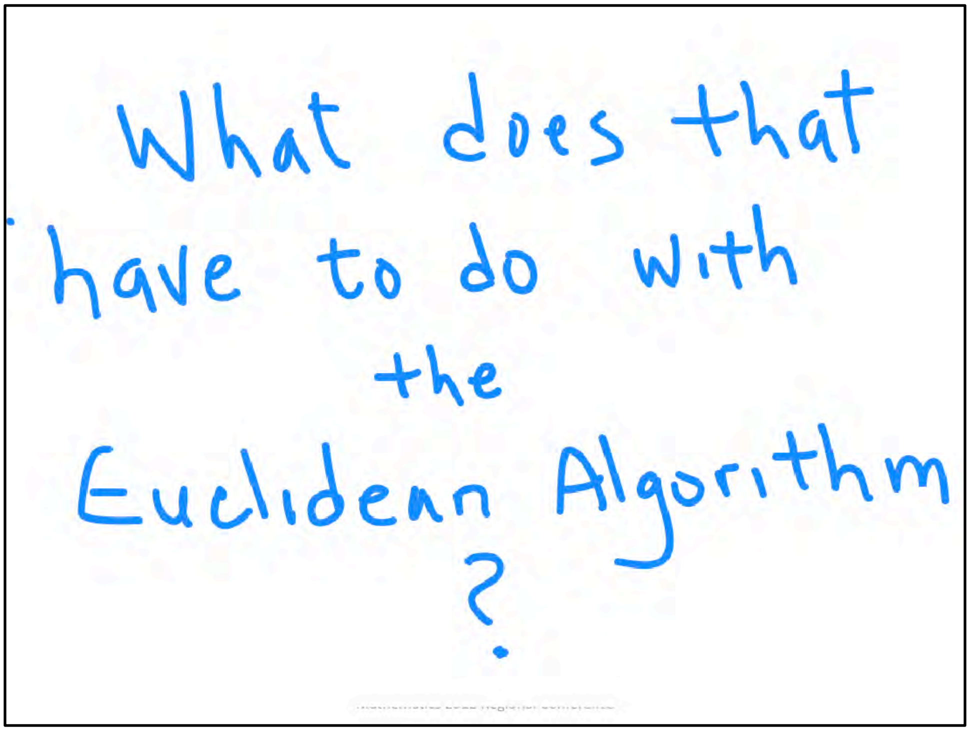
$$14 = 2 \cdot 7 \qquad 26 = 2 \cdot 13$$

$$14 \cdot 13 = 7 \cdot 2 \cdot 13 = 7 \cdot 26 \equiv 0 \bmod 26$$

but $14 \cdot 0 = 0$

Bad key

EXPLANATION: If a key (like 14) has a common factor (like 2) with 26. Then when we multiply 14 by a different factor of 26 (like 13) we end up with all factors of 26 (and other stuff, like 7) which makes a number equivalent to 0. But 14 times 0 is also zero so this is a bad key.



To see the connection, we will investigate how you decide what keys make GOOD keys.

Mod 26 Multiplication 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
1	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
2	00	02	04	06	08	10	12	14	16	18	20	22	24	00	02	04	06	08	10	12	14	16	18	20	22	24
3	00	03	06	09	12	15	18	21	24	01	04	07	10	13	16	19	22	25	02	05	08	11	14	17	20	23
4	00	04	08	12	16	20	24	02	06	10	14	18	22	00	04	08	12	16	20	24	02	06	10	14	18	22
5	00	05	10	15	20	25	04	09	14	19	24	03	08	13	18	23	02	07	12	17	22	01	06	11	16	21
6	00	06	12	18	24	04	10	16	22	02	08	14	20	00	06	12	18	24	04	10	16	22	02	08	14	20
7	00	07	14	21	02	09	16	23	04	11	18	25	06	13	20	01	08	15	22	03	10	17	24	05	12	19
8	00	08	16	24	06	14	22	04	12	20	02	10	18	00	08	16	24	06	14	22	04	12	20	02	10	18
9	00	09	18	01	10	19	02	11	20	03	12	21	04	13	22	05	14	23	06	15	24	07	16	25	08	17
10	00	10	20	04	14	24	08	18	02	12	22	06	16	00	10	20	04	14	24	08	18	02	12	22	06	16
11	00	11	22	07	18	03	14	25	10	21	06	17	02	13	24	09	20	05	16	01	12	23	08	19	04	15
12	00	12	24	10	22	08	20	06	18	04	16	02	14	00	12	24	10	22	08	20	06	18	04	16	02	14
13	00	13	00	13	00	13	00	13	00	13	00	13	00	13	00	13	00	13	00	13	00	13	00	13	00	13
14	00	14	02	16	04	18	06	20	08	22	10	24	12	00	14	02	16	04	18	06	20	08	22	10	24	12
15	00	15	04	19	08	23	12	01	16	05	20	09	24	13	02	17	06	21	10	25	14	03	18	07	22	11
16	00	16	06	22	12	02	18	08	24	14	04	20	10	00	16	06	22	12	02	18	08	24	14	04	20	10
17	00	17	08	25	16	07	24	15	06	23	14	05	22	13	04	21	12	03	20	11	02	19	10	01	18	09
18	00	18	10	02	20	12	04	22	14	06	24	16	08	00	18	10	02	20	12	04	22	14	06	24	16	08
19	00	19	12	05	24	17	10	03	22	15	08	01	20	13	06	25	18	11	04	23	16	09	02	21	14	07
20	00	20	14	08	02	22	16	10	04	24	18	12	06	00	20	14	08	02	22	16	10	04	24	18	12	06
21	00	21	16	11	06	01	22	17	12	07	02	23	18	13	08	03	24	19	14	09	04	25	20	15	10	05
22	00	22	18	14	10	06	02	24	20	16	12	08	04	00	22	18	14	10	06	02	24	20	16	12	08	04
23	00	23	20	17	14	11	08	05	02	25	22	19	16	13	10	07	04	01	24	21	18	15	12	09	06	03
24	00	24	22	20	18	16	14	12	10	08	06	04	02	00	24	22	20	18	16	14	12	10	08	06	04	02
25	00	25	24	23	22	21	20	19	18	17	16	15	14	13	12	11	10	09	08	07	06	05	04	03	02	01

Here's the multiplication table. It contains all the ciphers rows --- good and bad. If a row contains 1 it is a GOOD cipher – it will contain all numbers. That is because there is a number that "undoes" multiplication by that key.

	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
1	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
2	00	02	04	06	08	10	12	14	16	18	20	22	24	00	02	04	06	08	10	12	14	16	18	20	22	24
3	00	03	06	09	12	15	18	21	24	01	04	07	10	13	16	19	22	25	02	05	08	11	14	17	20	23
4	00	04	08	12	16	20	24	02	06	10	14	18	22	00	04	08	12	16	20	24	02	06	10	14	18	22
5	00	05	10	15	20	25	04	09	14	19	24	03	08	13	18	23	02	07	12	17	22	01	06	11	16	21
6	00	06	12	18	24	04	10	16	22	02	08	14	20	00	06	12	18	24	04	10	16	22	02	08	14	20
7	00	07	14	21	02	09	16	23	04	11	18	25	06	13	20	01	08	15	22	03	10	17	24	05	12	19

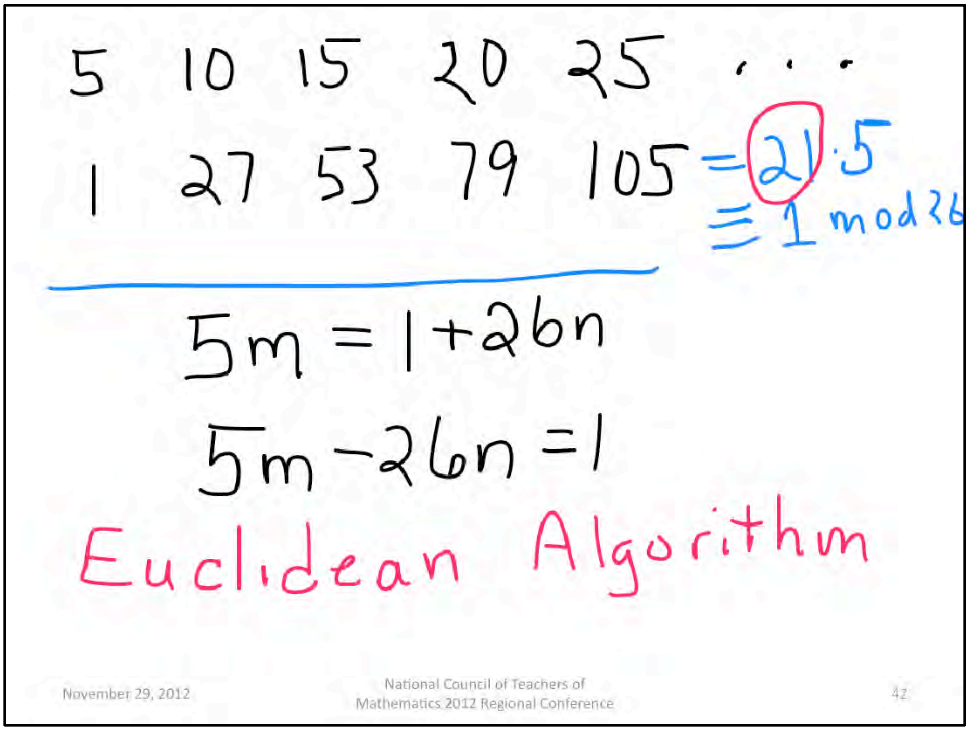
21 is the multiplicative inverse of 5:
multiplying by 21 “undoes” multiplying by 5.

To decrypt the times 5 cipher, multiply by 21

November 29, 2012 National Council of Teachers of Mathematics 2012 Regional Conference 41

As seen on the table, multiplying by 21 undoes multiplying by 5.

How can you determine if there is a multiplicative inverse (and what it is) if you don’t’ have the table?

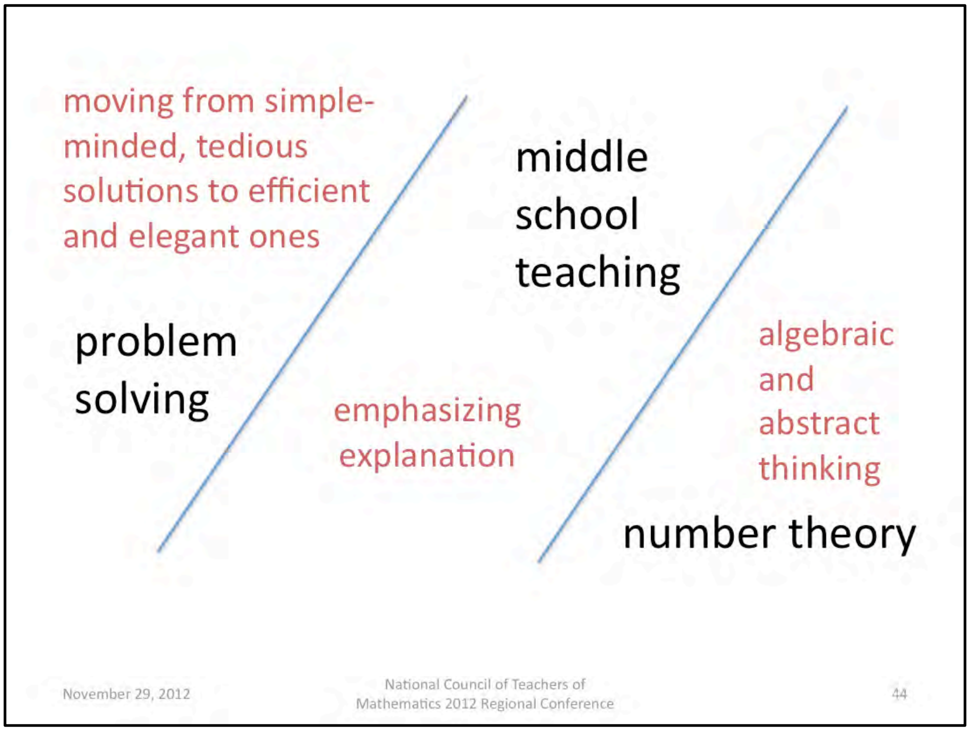


First start the times 5 cipher row (don't reduce this time). You want to find a number on this row that is equivalent to 1 mod 26. Those numbers, all on the same spoke of the wheel, look like 1 plus a multiple of 26.
Writing the algebra reveals that this is exactly the negative combination weight problem which we know two to solve.
Using the Extended Euclidean Algorithm we can find "m" and that will be the multiplicative inverse of 5.

Multiplicative Cipher key *k*

- Encrypt by multiplying by k mod 26
- Decrypt by multiplying by
  the multiplicative inverse of k mod 26
- Find the inverse of k
  by solving: $k \cdot m - 26 \cdot n = 1$

Summing up.



There are lots more examples of problems relating cryptography and middle school mathematics and Number Theory which I hope you will have time to explore. There are ways we can help.

Resources

Bonnie Saunders saunders@uic.edu

Materials for preservice and/or inservice course:
Problem Set, Project descriptions, syllabus, etc
Number Theory for Teachers workbook

Janet Beissinger beissing@uic.edu

For more information about CryptoClub Project and Summer Leader Workshop opportunities.

www.crcpress.com

The Cryptoclub: Using Mathematics to Make and Break Secret Codes
by Janet Beissinger and Vera Pless, CRC Press

cryptoclub.org

Under construction but has
lots of activities for students and others

The CryptoClub Project is funded by the National Science Foundation Grant # 0840313.
Prior funding was from NSF Grant # 0099220.

Pease fell free to be in touch.