NUMB3RS Activity: Creating Codes
Episode: "Backscatter"

Topic: Codes **Grade Level:** 10 - 12
Objective: Explore several coding methods
Time: 30+ minutes
Materials: TI-83/84 Plus calculator

Introduction

While lecturing to his students on backscatter analysis, Charlie finds a strange chunk of code embedded in the program he is discussing. The numbers in the coded message correspond to letters of the alphabet and warn him that "WE R WAITING FOR U."

Cryptography is the study of methods used to send messages in disguised form so only the intended recipients can decode and read the message. The message to be sent is the **plaintext** and the message in coded form is the **ciphertext.** The two main tasks in sending a coded message are coding (rewriting the plaintext in ciphertext) and decoding (translating the ciphertext into plaintext).

The crucial step is to develop **keys** – methods to create and read the ciphertext. In this activity we will discuss two simple letter-number substitution codes or ciphers and a simpler version of the code used to generate the message that Charlie received. One of these two simple codes is a **shift cipher** or **Caesar Cipher** (so named since they were used by Julius Caesar.) The code in the show used numbers generated by a "modular polynomial."

Discuss with Students

Most codes convert letters to numbers as the first step. Suppose each letter of the alphabet is assigned a position number from 1 to 26 as in the table below.

A	**B**	**C**	**D**	**E**	**F**	**G**	**H**	**I**	**J**	**K**	**L**	**M**
1	2	3	4	5	6	7	8	9	10	11	12	13
N	**O**	**P**	**Q**	**R**	**S**	**T**	**U**	**V**	**W**	**X**	**Y**	**Z**
14	15	16	17	18	19	20	21	22	23	24	25	26

A typical key is to "add 17" to form the ciphertext. In this case, B would be coded as 2 + 17 = 19. However, what would happen for the letter M? The value for M would be 13 + 17 = 30, which is greater than 26. In these cases, we need to use modular arithmetic. (Note that this discussion of modular arithmetic differs from the usual convention that would use 0 to 25 instead of 1 to 26.) A sum that exceeds 26 would be considered "modulo 26," so that M = 30 ≡ 4 mod 26. In general, for numbers *Z* that are not multiples of 26, *Z* mod 26 is the remainder when *Z* is divided by 26. When *Z* is a multiple of 26, *Z* mod 26 = 26.

Have students practice with modular arithmetic by answering the questions below.

1. Find each of the following numbers mod 26.
- **a.** 23
- **b.** 23 + 17
- **c.** 23 × 17
- **d.** 23^3

2. Numbers mod 26 can also be found using a calculator. To find the value of Z mod 26, compute $\boldsymbol{Z-26(\text{int}((Z-1)/26))}$. Use your calculator to check your answers to Question 1.

Discuss with Students Answers:
1a. 23 **1b.** 14 **1c.** 1 **1d.** 25

Student Page Answers:
1a. 25, 6, 24, 13, 16, 3, 4
1b. When $Z \neq 26k$, int $(Z/26)$ = int$((Z - 1)/26)$ is the quotient when Z is divided by 26. Then $Z - 26(\text{int}((Z - 1)/26))$ is the remainder. When $Z = 26k$, int$((Z - 1)/26) = k - 1$ so $Z - 26(\text{int}((Z - 1)/26)) = 26$.
1c. 24, 12, 5, 19, 16, 24, 12, 5, 20, 14, 4 (using L_1 = {13, 1, 20, 8, 5, 13, 1, 20, 9, 3, 19}, $L_2 = L_1 + 11$, and $L_3 = L_2 - 26(\text{int}((L_2 - 1)/26))$.

2. 14031001052618031201191O

3a. Coding a number n with the key **+11** and then decoding it with the key **+15** is equivalent to $n + 11 + 15 \equiv n$ mod 26. Coding and then decoding a number leaves it unchanged.
3c. PYTHAGORAS
3d. +(26 – *k*)

4a. 20110712041419112505241316020311160616020911170220151209
4b. ALL THE WORLD IS A STAGE

5a. 22071318190615
5b. Coding a number n with the key **×9** and then decoding it with the key **×3** is equivalent to $3(9n) = 27n \equiv n$ mod 26. Coding and then decoding a number leaves it unchanged.

6a. This key does not code every letter with a different number; for example 4 × 2 = 8 and 4 × 15 ≡ 8 mod 26, so the **×4** key would code both B and O as the same letter.
6b. the numbers relatively prime to 26: 3, 5, 7, 9, 11, 15, 17, 19, 21, 23, 25
6c. To decode a multiplicative cipher, the product of the coding key and decoding key must be ≡ 1 mod 26. This ensures that coding and then decoding a number n will be equivalent to n mod 26. (For example, 11 × 19 = 209 ≡ 1 mod 26, so coding a number n the **×11** key and then decoding it with the **×19** key would give $n \times 11 \times 19 \equiv n$ mod 26.) The valid pairs of coding/decoding keys are listed below:
×3 and **×9**, **×5** and **×21**, **×7** and **×15**, **×9** and **×3**, **×11** and **×19**, **×15** and **×7**, **×17** and **×23**, **×19** and **×11**, **×21** and **×5**, **×23** and **×17**, **×25** and **×25**

7a. Possible answer: $b = 29$, $c = 11$; another is $b = -8$, $c = 48$ or 11; Then $p(x) = 17x^3 + 29x^2 + 11x$ and $\{p(1), p(2), p(3)\} = \{57, 274, 753\} \equiv \{20, 15, 13\}$ mod 37 = TOM
7b. Answers vary.

Tom Butts, UT Dallas

Name: _____ Date: _____

NUMB3RS Activity: Creating Codes

While lecturing to his students on backscatter analysis, Charlie finds a strange chunk of code embedded in the program he is discussing. The numbers in the coded message correspond to letters of the alphabet and warn him that "WE R WAITING FOR YOU."

Cryptography is the study of methods used to send messages in disguised form so only the intended recipients can decode and read the message. The message to be sent is the **plaintext** and the message in coded form is the **ciphertext.** The two main tasks in sending a coded message are coding (rewriting the plaintext in ciphertext) and decoding (translating the ciphertext into plaintext).

The crucial step is to develop **keys** – methods to create and read the ciphertext. The first step is to assign a number from 1 to 26 to each letter of the alphabet as in the table below.

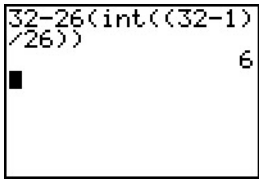
A	**B**	**C**	**D**	**E**	**F**	**G**	**H**	**I**	**J**	**K**	**L**	**M**
1	2	3	4	5	6	7	8	9	10	11	12	13
N	**O**	**P**	**Q**	**R**	**S**	**T**	**U**	**V**	**W**	**X**	**Y**	**Z**
14	15	16	17	18	19	20	21	22	23	24	25	26

1. One common key is the **additive cipher**, where every plaintext letter is replaced by a number that is a fixed amount greater than its number in the table. Suppose we wish to code the word "NUMBERS" using the **+11 key**. The letter N would become 14 + 11 = 25. However, when we try to code the letter U, we get 21 + 11 = 32. Because no letter will correspond to 32 when the message is later translated, how can we code this message?

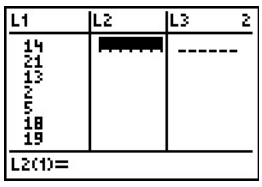
To code the message, we consider all numbers modulo 26 so that U = 32 ≡ 6 mod 26. In general, for numbers Z that are not multiples of 26, Z mod 26 is the remainder when Z is divided by 26. When Z is a multiple of 26, Z mod 26 = 26.

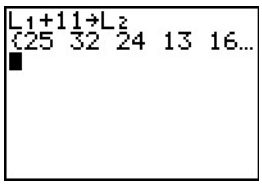
a. Complete this coding of the word NUMBERS**:** 25, 6, __, __, __, __, __ **.**

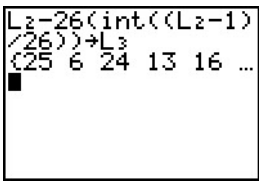
b. Explain why you could code each letter Z using the formula Z mod 26 = Z – 26(int((Z – 1)/26)), where int(Z) is the greatest integer less than or equal to Z. The calculation for U = 32 is shown below.

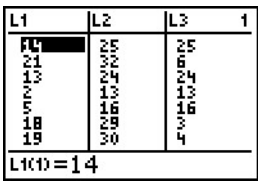


In fact, you could manipulate lists and do the entire coding of "NUMBERS" using the **+11** key on a TI-83/84 as shown below.









c. Use your calculator to code the word MATHEMATICS using the **+11** key.

Sometimes we assign every letter a 2-digit number and code the message without spaces.

A	**B**	**C**	**D**	**E**	**F**	**G**	**H**	**I**	**J**	**K**	**L**	**M**
01	02	03	04	05	06	07	08	09	10	11	12	13
N	**O**	**P**	**Q**	**R**	**S**	**T**	**U**	**V**	**W**	**X**	**Y**	**Z**
14	15	16	17	18	19	20	21	22	23	24	25	26

In this case the **+11** code for "NUMBERS" would be 25062413160304.

2. Find the **+11** code for the word CRYPTOGRAPHY in this form.

3. **a.** If we received the code 25062413160304, we would decode it using the **+15** key. Why?

b. Decode this message by adapting the calculator routine above using the **+15** key and verify that you obtain 14211302051819 or "NUMBERS."

c. Decode the message 01100519121826031204 assuming it was sent with the **+11** key.

d. If we used the **+k** key to code a message, what key would we use to decode the message?

4. It can be awkward to send a message with commas and for messages with more than one word it might be hard to read using the coding system in Question 2. Therefore, many people add a space to separate words and assign it the number 27.

A	**B**	**C**	**D**	**E**	**F**	**G**	**H**	**I**	**J**	**K**	**L**	**M**
01	02	03	04	05	06	07	08	09	10	11	12	13
N	**O**	**P**	**Q**	**R**	**S**	**T**	**U**	**V**	**W**	**X**	**Y**	**Z**	
14	15	16	17	18	19	20	21	22	23	24	25	26	27

a. Code the phrase I WATCH NUMBERS EVERY FRIDAY using the **+11** key with the space added. [Hint: Remember to use mod 27.]

b. Decode the coded message below, assuming it was sent with the **+11** key.
1223231104191611072602231511200311121103041218 16

5. Return to the original table without the space [mod 26]. Another common key is the **multiplicative cipher** where every plaintext letter is replaced by a number is that is the product of a fixed number and the number in the table. Suppose we wish to code the word "NUMBERS" using the **×9** key. Then N = 14 would be coded as 22 (because 9 × 14 = 126 ≡ 22 mod 26).

a. Complete the coding of NUMBERS using the **×9** key.
22, __, __, __, __, __, __ .
[Hint: Adapt the calculator routine used for the **+11** key.]

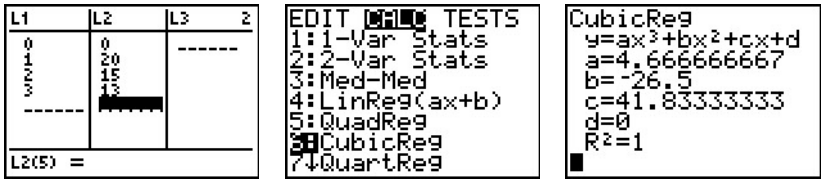
b. To decode a message sent with the **×9** key, we would use the **×3** key. Why? [Hint: 9 × 3 = 27 ≡ 1 mod 26] Decode your message from part a, and verify that the word NUMBERS was sent.

6. a. A **×4** key would **not** be a valid multiplicative cipher. Why? [Hint: Think of the results you would get if you tried to use a **×4** key.]

b. What numbers *N* between 1 and 26 could be used as a **×*N*** coding key? Why?

c. For each valid **×*N*** coding key found in part b, find the corresponding decoding key. [Hint: Think of your result from Question 5b.]

7. Challenge The message in the episode, "WE R WAITING FOR U", was received as {23, 5, 18, 23, … } mod 37 – the output of a "modular polynomial" of degree 14, whose constant term was 0 and whose input was {1, 2, 3, …, 14}. To send the message of the name "TOM" would require a polynomial of degree 3 whose constant term is 0 and whose graph would contain the points (0, 0), (1, 20), (2, 15), and (3, 13). (Recall that T = 20, O = 15, and M = 13.) We can find such a polynomial using **CubicReg** on the TI-83/84 Plus calculator, as shown below.



The coefficients are rational numbers that we wish to convert to integers mod 37. We have $a = \frac{14}{3}$, $b = -\frac{53}{2}$, and $c = \frac{251}{6}$.

To convert a to a positive integer mod 37, we seek a value of x so that $\frac{(14 + 37x)}{3}$ is an integer. One of the infinitely many possible choices is $x = 1$ and $a = 17$.

a. Find values of b and c for this polynomial and check that the inputs {1, 2, 3} yield the message "TOM."

b. Choose a 3 or 4 letter name and find an associated polynomial with constant term 0 that could be used to code that name mod 37 using the inputs {1, 2, 3} or {1, 2, 3, 4}. Check your answer.

The goal of this activity is to give your students a short and simple snapshot into a very extensive math topic. TI and NCTM encourage you and your students to learn more about this topic using the extensions provided below and through your own independent research.

Extensions

For the Student

1. Consider the table below.

A	B	C	D	E	F	G	H	I	J	K	L	M
01	02	03	04	05	06	07	08	09	10	11	12	13
N	**O**	**P**	**Q**	**R**	**S**	**T**	**U**	**V**	**W**	**X**	**Y**	**Z**	
14	15	16	17	18	19	20	21	22	23	24	25	26	27

a. If we used the **+k** key to code a message, what key would we use to decode the message?
b. What numbers *N* between 1 and 27 could be used as a **×*N*** coding key? Why?
c. For each valid **×*N*** coding key found in part b, find the corresponding decoding key.

2. In Question 6b of the student activity, we learned that **×*N*** was a valid key when *N* was relatively prime to 26. In general, the number of integers that are less than *n* and relatively prime to *n* is denoted by $\varphi(n)$ and is called the Euler-Phi function. This function plays a crucial role in the RSA code (a "public-key" code which is very hard to break and does **not** require that both parties agree on a coding and decoding method). Research the RSA code and other similar public-key codes.

Additional Resources

In Code: A Mathematical Journey, Sarah Flannery, David Flannery, Workman Publishing, 2001

This DVD, "Discrete Math: Cracking the Code," contains an introduction to methods of electronic information transmission including public-key cryptography.
http://www.comap.com/product/?idx=582

Simon Singh has written a very readable book entitled *The Code Book: How to Make It, Break It, Hack It, Crack It*. This companion Web site has many pages on the history and uses of cryptography.
http://www.simonsingh.net/The_Black_Chamber/contents.htm

This interactive math applet from NCTM's Illuminations can be used to explore math and create interactive lessons. This applet allows you to explore a substitution cipher by encoding and decoding text messages. Shift transformation and the stretch value are introduced.
http://illuminations.nctm.org/tools/tool_detail.aspx?id=5

"An Overview of Cryptography", by Gary Kessler, can be viewed at the Web site below.
http://www.garykessler.net/library/crypto.html

Tom Butts, UT Dallas