Using Cryptology to Stimulate the Student's Interest in Mathematics Through Applications of Functions and Their Inverses

Carlos G. Spaht, II, W. Conway Link, and Rogers Martin

Mathematics Department
Louisiana State University in Shreveport

Abstract

With recent media attention focusing on the importance of maintaining secure lines of communication, it may be a good time to introduce simple cryptology examples in your math based courses as a means of stimulating student's interest in mathematics. Examples discussed in this paper have been presented to students with a wide range of mathematical abilities from middle school to senior level college math students.

Using cryptology as a teaching tool allows the instructor to demonstrate the existence of a variety of functions and their inverses. If the instructor feels comfortable discussing some counting principles and probability concepts, cryptology can be made to be more meaningful. The most important benefit, is that some students see for the first time practical and important real-world applications for some of the mathematics they have been studying.

Encryption of plaintext using matrices as presented in LaPREP, a nationally acclaimed engineering, math, and sciences enrichment program for middle school students held on the LSU-Shreveport campus, has already been reported in the 1999 ASEE GSW Conference Proceedings[4]. This encryption procedure has also been used as an application of mathematics in College Algebra, Discrete Math, and Linear Algebra classes at LSUS.

Cryptology also provides excellent examples of applications of modular arithmetic for Abstract Algebra and Discrete Math students. This paper will focus on examples of cryptology using modular arithmetic.

Introduction

The concept of function is one of the most important concept in mathematics, yet a recent evaluation of post College Algebra mathematics students yielded an unexpected high percentage who were unable to correctly define "function" and to correctly solve a literal equation for one unknown as a function of the others. If courses are taken in their normal sequence, by the time a student enrolls in a calculus course, they will have been exposed to linear, polynomial, rational, exponential, logarithmic, and trigonometric functions. Piece-wise defined functions, which are sometimes introduced in College Algebra and revisited in calculus, are difficult for some to grasp since more than one equation is required in the definition.

Unless enrolled in a Discrete Math or Probability course, a student may never be exposed to the wide variety of functions available for study. Using encryption and decryption to illustrate examples of functions may be worthwhile for several reasons: (1) recent terrorist activities have increased the public's awareness of the need to keep secret messages secure; (2) there has been a growing interest in cryptology among adults since 1990. This claim is supported in part by the popularity of books such as Seizing the Enigma (David Kahn, 1991), The Code Book (Simon Singh, 1999), Station X – Decoding Nazi Secrets (Michael Smith, 1999), The Bible Code (Michel Drosnin (1997), and Cracking the Bible Code (Jeffrey Satinover, 1997); (3) for more than 60 years, cartoonists have presented encoding and decoding ideas to children through comic strips such as Herge's 1947 Les Aventures de Tintin – Le Secret de La Licorne (French Text) and Carl Bark's Search for the Cuspidoria (Walt Disney's Comics and Stories, January 1955). Some cartoon characters actually had their own coding and decoding units available for their youthful readers -- Little Orphan Annie had Secret Decoder Rings in the 1930s and Captain Midnight's Secret Code Book and Membership Manual and Decoder Badges were available in the early 1940s (4) some applications of mathematics appeal to a wider audience than others. Students seem to find uniform motion problems, painter problems, and mixture problems rather boring, but perk up a little when the relationship between the study of ellipses and the construction of a lithotripter is explained. They see the likelihood of being asked to solve a painter or mixture problem in real life as remote, whereas they probably know someone who has experienced the kidney stone phenomena and can therefore appreciate the application of an analytic geometry concept being used to solve a real world problem.

To address both the need to have real world examples and to appeal to the student's interest in cryptology, some authors have included easy-to-understand examples of encryption in their college level math texts (College Algebra, Linear Algebra, Number Theory, and Discrete Math). These examples are sometimes restricted to the use of linear functions or square matrices for enciphering[3]. However, with just a little time devoted to the fundamentals of modular arithmetic, the student's exposure to and understanding of both cryptology and functions can be expanded considerably.

Encoding For Error Detection and Correction

Introduction

Messages are seven binary digits long and consist of two parts: a four digit data part, d1d2d3d4, and a three digit error check part, c1c2c3. Errors occur when messages are corrupted during transmission, a 0 is received as a 1, or a 1 is received as a 0[3].

Messages are encoded using parity check sums. Parity, the number of 1 digits in a message, can be either even or odd. A check sum is the sum of the digits being examined[1]. In this paper, parity will be even. Even parity is determined using the mod function, which is the remainder in a division problem. For example, $6 \bmod 2 = 0$, because 6 divided by 2 equals 3 with a remainder of 0.

Encoding

The domain of the encoding function consists of the set of four digit strings holding the data. The range of the encoding function is the set of seven digit strings, where each string is composed of four data digits followed by three check digits, d1d2d3d4c1c2c3. The check digits are appended to the four data digits according to the following rules:

$C1 = 0$ if $(d1 + d2 + d3) \bmod 2 = 0$
$C1 = 1$ if $(d1 + d2 + d3) \bmod 2 \neq 0$;

$C2 = 0$ if $(d1 + d3 + d4) \bmod 2 = 0$
$C2 = 1$ if $(d1 + d3 + d4) \bmod 2 \neq 0$; and

$C3 = 0$ if $(d2 + d3 + d4) \bmod 2 = 0$
$C3 = 1$ if $(d2 + d3 + d4) \bmod 2 \neq 0$.

This is the encoding function.

Example 1:

Encode 1010.

$d1 = 1, d2 = 0, d3 =1, d4 = 0$

For c1, $(d1 + d2 + d3) \bmod 2 =$
$(1 + 0 + 1) \bmod 2 =$
$2 \bmod 2 = 0$
Thus, $c1 = 0$.

For c2, $(d1 + d3 + d4) \bmod 2 =$
$(1 + 1 + 0) \bmod 2 =$
$2 \bmod 2 = 0$
Thus, $c2 = 0$.

For c3, $(d2 + d3 + d4) \bmod 2 =$
$(0 + 1 +0) \bmod 2 =$
$1 \bmod 2 = 1$

Thus, $c3 = 1$.

The encoded message is 1010001.

Decoding

The decoding function maps a seven digit string d1d2d3d4c1c2c3 back to a four digit string d1d2d3d4 by examining the check digits and the data digits. The decoding function is:

```
If (d1 + d2 + d3 + c1) mod 2 = 0 then
    d1, d2, d3 are error free.
If (d1 + d2 + d3 + c1) mod 2 ≠ 0 then
    d1, d2, d3 contains an error.

If (d1 + d3 + d4 + c2) mod 2 = 0 then
    d1, d3, d4 are error free.
If (d1 + d3 + d4 + c2) mod 2 ≠ 0 then
    d1, d3, d4 contains an error.

If (d2 + d3 + d4 + c3) mod 2 = 0 then
    d2, d3, d4 are error free.
If (d2 + d3 + d4 + c3) mod 2 ≠ 0 then
    d2, d3, d4 contains an error.
```

Example 2:

Decode 1100110.

d1 = 1, d2 = 1, d3 = 0, d4 = 0, and
c1 = 1, c2 = 1, c3 = 0

Examine the first check sum.
(d1 + d2 + d3 + c1) mod 2 =
(1 + 1 + 0 + 1) mod 2 =
3 mod 2 = 1

Thus, the first check sum contains an error.

Examine the second check sum.
(d1 + d3 + d4 + c2) mod 2 =
(1 + 0 + 0 + 1) mod 2 =
2 mod 2 = 0

Thus, the second check sum is error free.

Examine the third check sum.
(d2 + d3 + d4 + c3) mod 2 =
(1 + 0 +0 + 0) mod 2 =
1 mod 2 = 1
Thus, the third check sum contains an error.

Error location begins with the recognition that each data digit is part of two check sums. If the set of digits used to compute each erroneous check sum is compared, a small set of possible error digits is found. Then, the set of possible error digits is compared to the set of digits in the error free check sum. This leaves only a single digit as the error digit.

Example 3:

Locate the error in 1100110.

From Example 2, c1 contains an error, c2 is error free, and c3 contains an error. Let s1 be the data digits in c1, s1 = {d1, d2, d3}. Let s2 be the data digits in c2, s2 = {d1, d3, d4}. Let s3 be the data digits in c3, s3 = {d2, d3, d4}. Since c1 and c3 contain errors, examine s1 and s3 for common error digits, by examining s1 ∩ s3. This produces a set of possible error digits, {d2, d3}. Next, intersect this set with the error free set s2. The result of this operation is {d3}, which is a member of set that is error free. Remove d3 from the set of possible error digits. Thus, the error digit is d2.

Example 4.

Correct the error digit in 1100110.

The error digit is d2, which is 1. If a digit of 1 is incorrect, then the correct value for that digit is 0. The corrected message is 1000110.

Ciphers Using Modulo Arithmetic

An early form of a cipher was used by Julius Caesar during the Gallic wars[2]. In this system, he simply replaced each letter (the plaintext) by a letter by a letter three units to the right (the ciphertext).

A substitution of our alphabet would appear as follows:

Plaintext: A B C D E........W X Y Z
Ciphertext: D E F G H........Z A B C

The plaintext message "STRIKE" would be encoded and decoded using the substitution alphabet.

Plaintext: S T R I K E
Ciphertext: VWU L NA

Ciphers can be described mathematically. First we adopt the following notational convention and list a few basic properties of modulo arithmetic:

Mod[a,n] is the remainder when a is divided by n. That is,
Mod[a,n] = r if and only if there exist integers q and r such
that $a = nq + r$ where $0 \le a < n$.
Frequently [a] will be used to denote Mod[a,n] if the value of n is understood. Note that
[a] = a if $0 \le a < n$.

Example 1:

Mod[25,7]=4, Mod[7,25]=7 and Mod[63,21]=0. Also, if n = 27, then [48] = 21, [55] = 1 and [100] = 19.Also since [a] = a if 0 β a < n, we can write
Mod[25,7] = [4], Mod[7,25] = [7], etc.

Elementary properties of Mod[a,n] = [a]:

(1) [a] = [b] if and only if n divides (a - b), i.e., if and only if a - b = kn for some integer k. (This is easy to see by letting a = nq + r and b = nq' + r' where $0 \le r,r' < n$, and then studying a - b = n(q - q') +(r - r').)

(2) [-x] = [n - x].
(This follows immediately from part (1).)

(3) [a] = [b] implies both [a ± c] = [b ± c] and [ac] = [bc] for any integer c.
(This is clear.)

(4) If [a] = [b] and [d] = [e], then [a + d] = [b + e] and [ad] = [be].
(Since [a] = [b] and [d] = [e], there exist integers k and l such that
a - b = kn and d - e = ln. Thus, (a + d) - (b + e) = (k + l)n and
[a + d] = [b + e].We also have that ad - bd = (kd)n and
bd - be = (le)n. Consequently, (ad - bd) +(bd - be) = ad - be = (kd + le)n
and therefore, [ad] = [be].)

(5) If the greatest common divisor of a and n, denoted gcd(a,n), is equal to 1, then there exists an integer a^{-1} such that $0 < a^{-1} < n$ and $[aa^{-1}] = [1] = 1$.
(Since gcd(a,n) =1, by the Euclidean Algorithm there exist integers s and t such that as + tn = 1. Thus, (as) -1 = n(-t) , and therefore, [as] = [1] = 1. Now chose a^{-1} such that $a^{-1} =$ [s]. Since $a^{-1} = [a^{-1}]$ =[s], then by property 4 above, $[aa^{-1}]$ = [as] =1.)
[Note that the converse of property (5) is also true. For if $[aa^{-1}] = 1 = [1]$ for some integer a^{-1}, then $aa^{-1} - 1 = kn$ for some integer k. Thus, $aa^{-1} + (-k)n = 1$ which means that $\gcd(a^{-1},n) = 1$.]

(6) Assume that A = {1,2,3,....,n} and f : A --> A given by
c = f (p) = [ap + b] where gcd(a,n) = 1. (It will become clear in a moment why we are using p and c instead of x and y for the variables of this function.) Then f has an inverse defined by p = f^{-1}(c) = [a^{-1}(c - b)] where a^{-1} is the integer as described in property (5) above.
(If c = [ap+ b], then [c] = [ap + b]. Thus,

$$[c - b] = [ap] \text{ and}$$
$$[a^{-1}(c - b)] = [p].$$

Therefore, p = f^{-1}(c) = [a^{-1}(c - b)].)

Let's now continue our discussion of ciphers by describing one using this modulo arithmetic. We will associate the n letters of the alphabet with the n nonnegative integers A={0,1,2,3,....,n-1} and define a mapping f:A→A by the encryption function c = f(p)=Mod[p +k,n], where k is the key, the number of positions from the plaintext to the ciphertext. For example with Caesar's cipher, since there is a shift of 3 letters to the right, k = 3.

To illustrate Caesar's cipher as well as the other examples in this paper, we will use the following alphanumeric cipher:

BLANK 0

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

For Caesar's message, our ciphered message becomes

plaintext→	S	T	R	I	K	E
p-numbers→	19	20	18	9	11	5
c-numbers (c= Mod[p+3,27])→	22	23	21	12	14	8
ciphertext→	V	W	U	L	N	H

To decipher the messages, we use the inverse functions. From property 6 above, we see that if c = [p+k], then its inverse is given by p = [x-k] (In this case, both a and a^{-1} are equal to one. Thus, the ciphered message VWULNH can be deciphered as follows:

ciphertext→	V	W	U	L	N	H
c-numbers→	22	23	21	12	14	8
p-numbers (p= [c-3])→	19	20	18	9	11	5
plaintext→	S	T	R	I	K	E

Example 2:

For a more sophisticated example, let's choose the mapping
c = Mod[5p + 7,27] = [5p + 7]over our 27 letter alphabet. The message STRIKE would be encoded as follows:

plaintext→	S	T	R	I	K	E
p-numbers→	19	20	18	9	11	5
c-numbers (c= [5p+7])→	21	26	16	25	8	5
ciphertext→	U	Z	P	Y	H	E

To decode this message, we would apply the inverse of c = [5p + 7]. From properties listed above, we have the following:

$$
\begin{aligned}
[c] = [5p+7] &\Rightarrow [c-7] = [5p] \\
&\Rightarrow [5^{-1}(c-7)] = [p].
\end{aligned}
$$

$$
\begin{aligned}
\therefore p &= [5^{-1}(c-7)] \\
&= [11(c-7)] \quad \text{(since } [5]*[11] = [1]\text{)} \\
&= [11(c+20)] \quad \text{(since } [-7] = [27-7] = [20]\text{)} \\
&= [11c + 220] \\
&= [11c + 4] \qquad \text{(since } [220] = [4]\text{)}
\end{aligned}
$$

The message UZPYHE can now be deciphered as follows:

ciphertext→	U	Z	P	Y	H	E
c- numbers→	21	26	16	25	8	5
p- numbers (p = [11c + 4]) →	19	20	18	9	11	5
plaintext→	S	T	R	I	K	E

Example 3:

Use c=f(p) = [p + 15] to encode and decode the message HELP. We first encode the message:

plaintext→	H	E	L	P
p-numbers→	8	5	12	16
c-numbers (c= [p+15])→	23	20	0	4
ciphertext→	W	T	B	D

Now to decode the message :

ciphertext→	W	T	B	D
c-numbers→	23	20	0	4
p-numbers (p = [c - 15]) →	8	5	12	16
plaintext→	H	E	L	P

Example 4:

Use c = [2p + 7] to encode and decode the message HELP. First to encode the message:

plaintext→	H	E	L	P
p-numbers→	8	5	12	16
c-numbers (c= [2p+7])→	23	17	4	12
ciphertext→	W	Q	D	L

To decode the message we first find the inverse of c = [2p + 7]:

$$
\begin{aligned}
[c] = [2p + 7] &\Rightarrow [c - 7] = [2p] \\
&\Rightarrow [2^{-1}(c - 7)] = [p] \\
&\Rightarrow [14c - 7)] = [p] \quad (\text{ since } [2][14] = [1]) \\
&\Rightarrow [14c - 98] = [p] \\
&\Rightarrow [14c + 10] = [p] \quad (\text{ since } -98 = 4*27 + 10) \\
&\Rightarrow [p] = [14c + 10].
\end{aligned}
$$

We now decode the message:

ciphertext→	W	Q	D	L
c-numbers→	23	17	4	12
p-numbers (p = [14c + 10]) →	8	5	12	16
plaintext→	H	E	L	P

Summary and Conclusions

For many years, encryption and decryption using matrices has been a staple in the Discrete Math component of LaPREP. When doing end-of-course evaluations, students ranked this as their favorite topic above other applications including stochastic matrices and “0-1” matrices. In this paper, applications of cryptography using functions incorporating modular arithmetic for both error checking and ciphers have been discussed. Cryptology provides excellent examples of modular arithmetic for Abstract Algebra and Discrete math classes. Such applications are now being included in these classes at LSUS and the students have found them to be of great interest. Many have gained a new appreciation for mathematics and have expressed an interest in forming a campus cryptology organization.

References

1. Gallian, Joseph. “Chapter 10: Transmitting Information.” For All Practical Purposes: Introduction to Contemporary Mathematics. Edited by Solomon Garfunkel. 5th ed. New York: W. H. Freeman and Company, 2000.
2. Gilbert, Jimmie, and Gilbert, Linda. Elements of Modern Algebra. 5th ed. Pacific Grove, CA: Brooks/Cole, 2000.
3. Kolman, Bernard; Busby, Robert C.; and Ross, Sharon Cutler. Discrete Mathematical Structures. 4th ed. Upper Saddle River, NJ: Prentice Hall, 2000.
4. Link, Conway, and Spaht, Carlos. “LaPREP: A Highly Successful Enrichment Program and its Discrete Math/Probability and Statistics Components.” The Proceedings of the 1999 American Society of Engineering Education Gulf Southwest Annual Conference, 1999, on CD-ROM.

CARLOS G. SPAHT, II
Dr. Spaht serves as Professor of Mathematics at Louisiana State University in Shreveport. For several years he has raised funds for and directed LaPREP, a nationally acclaimed intervention program in engineering, math and science for high-ability middle and early high school students. His research interests include intervention programs and Abstract Algebra.

W. CONWAY LINK
Mr. Link serves as an Assistant Professor of Mathematics at Louisiana State University in Shreveport. Since 1985, he has developed and coordinated programs for academically talented students and has taught the probability/statistics and discrete math components of LaPREP. His research interests include statistics and education.

ROGERS MARTIN
Mr. Martin serves as Instructor of Mathematics at Louisiana State University in Shreveport. For several years, he has taught algebra and discrete math classes. His research interests include applied math, computer science, and education.