The Report Committee for Ariel Jolishia Taylor
certifies that this is the approved version of the following report:

Practicality of Algorithmic Number Theory

APPROVED BY
SUPERVISING COMMITTEE:

Supervisor: ________________________________
John Luecke

____
Mark Daniels

Practicality of Algorithmic Number Theory

by

Ariel Jolishia Taylor, BS

Report

Presented to the Faculty of the Graduate School of

The University of Texas at Austin

in Partial Fulfillment

of the Requirements

for the Degree of

Master of Arts

The University of Texas at Austin
August 2013

Dedication

This report is dedicated to my Aunt Shelia Tyler.

Acknowledgements

Special thanks and acknowledgements to my parents, Alethea and Ruiel Taylor III, my siblings, Dominique Tyler, Muriel Taylor and Ruiel Taylor IV, and my inspiring high school math teacher, Dr. Carol Holmes.

Abstract

Practicality of Algorithmic Number Theory

Ariel Jolishia Taylor, MA

The University of Texas at Austin, 2013

Supervisor: John Luecke

This report discusses some of the uses of algorithms within number theory. Topics examined include the applications of algorithms in the study of cryptology, the Euclidean Algorithm, prime generating functions, and the connections between algorithmic number theory and high school algebra.

Table of Contents

List of Tables

List of Figures

Chapter 1: An Introduction

Number theory is a branch of pure mathematics that studies the properties of integers. *Algorithmic number theory* is the study of algorithms used to perform specific number theory computations. This involves finding solutions to equations, proving their existence and non-existence, and making efficient use of resources such as time and space. General examples include the listing of primes, determining the greatest common divisor (GCD) of two integers using concepts of divisibility, and investigating the sum of high powers as in *Fermat's Last Theorem.*

The fact that linear congruence of integers in modular arithmetic is analogous to solving linear equation in elementary algebra is commonly unnoticed. Most secondary algebra teachers fail to make a connection between abstract algebra and number theory in the high school mathematics curriculum. This disconnect is transferred to students and therefore carried to college. Integer computations in number theory algorithms are based on elementary algebra concepts. A congruence of the form

$$a \equiv b \pmod{n} \text{ where } a, b, n \in \mathbb{Z}$$

can be rewritten as

$$a = b + nk \text{ where } k \in \mathbb{Z}.$$

By connecting these forms, students can be provided with a stronger introductory understanding of algorithmic number theory in high school algebra.

Number theory is appreciated by mathematicians for its purity and beauty but rarely by non-mathematicians for its practicality. One use for algorithmic number theory is that it is important in establishing codes for reliable and secure information transmission. *Cryptography*, the art and study of making communication unintelligent to all except the intended recipients, is an interesting growing mathematical phenomenon.

Cryptography is the complete science of secure communication; it integrates algorithmic mathematical number theory, engineering, and computer science. All of which are increasingly necessary fields of study in this century. Cryptography is not new; it has been studied and used since before 100 B.C for diplomatic purposes with Julius Caesar. Today, there is an urgent need to provide cost-effective, efficient, and secure systems to protect the vast quantity of digital data stored and communicated by electronic data-processing systems. [**2**, p. 1]. In order to further the advancement of technology and information security, students must acquire 21st century skills*,* the skills needed to succeed in learning, working, and living in this century.

In the following chapters, specific algorithms are examined and investigated. The ability and necessity for these algorithms to be taught within secondary education is highlighted.

Chapter 2: Ciphers in Cryptanalysis

A *cipher* is a method which transforms plaintext into ciphertext by applying a set of transformations onto each character in the plaintext. A cipher is an algorithm, and depending on the strength of the algorithm, through cryptanalysis, a ciphertext can be attacked and decrypted. An encryption function is used to produce ciphertext from plaintext. With E, the encryption function, P, the plain text, and $C,$ the ciphertext,

$$E(P) = C.$$

The decryption function determines the plaintext from the ciphertext. With $D,$ the decryption function, $D(C) = P$. An encryption key is a piece of data that allows for the computation of E. Similarly there is a decryption key. These keys may be public or private.

Linear ciphers such as the *Ceasar Cipher* have been proved extremely insecure. Ceasar Cipher, which dates back to around 50 B.C., assigns each letter of the alphabet a double digit number 00-25 modulo 26. The alphabet then shifts three places to the right and loops around to the beginning. For example,

$$25 + 3 = 02, Z \rightarrow C.$$

$$E(P) = P\ + 3\ (mod\ 26)\ =\ C,$$

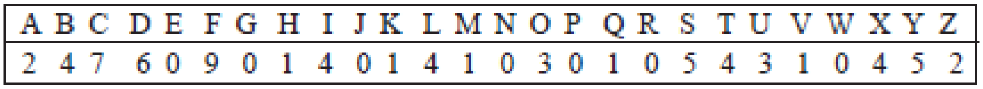
$$D(C) = C + 23\ (mod\ 26)\ = P.$$

The ability to understand linear congruences and to write linear equations is necessary prerequisite knowledge in order to engage in the study of information security. Consider the ciphertext:

XHTQF SCUFD SBULX IOLBF ALYZT IDSCL
YCSDO FZYCU FAFMF ODITF YCDKV SBICD
XBXCF TX

Asuuming the ciphertext is of the general form of a linear Ceasar Cipher modulo 26, a frequency distribution of the letters in the English Language alphabet can be used to determine the linear cipher key used in encryption. Table 1 shows the frequency distribution of the letters in the ciphertext presented.

Table 1. Frequencies of letters in the ciphertext [**2**, p. 3].



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
2	4	7	6	0	9	0	1	4	0	1	4	1	0	3	0	1	0	5	4	3	1	0	4	5	2

The letters *E* and *T* have the highest frequency in the English Language as shown in Table 2, so it is hypothesized that since *F* and *C* have the highest frequency in the ciphertext that they are corresponding characters respectively. Assuming E, the encryption function modulo 26, is of the general form of the linear Ceasar Cipher, we have,

$$E(4) = 5, and\ E(19) = 2,$$

that is;

$$4k\ + t\ = 5\ (mod\ 26) \text{ and } 19k + t = 2\ (mod\ 26) \text{ for } k, t\ \in\ \mathbb{Z}\,.$$

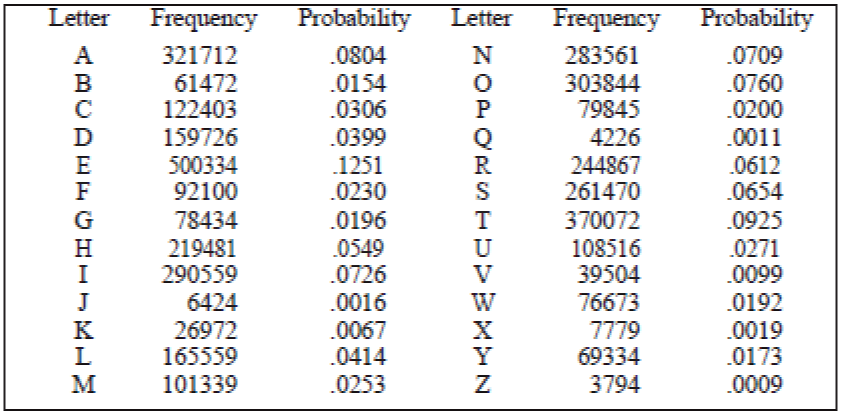
Using methods of solving systems of equations, it is determined $k\ =\ 5$, and $t\ =\ 11$. Therefore the conjectured encryption function is

$$E(P) = 5(P) + 11\ (mod\ 26).$$

The decryption function is determined from the additive and multiplicative inverse functions modulo 26.

$$D(C) = 21(C + 15)\ (mod\ 26).$$

Table 2. Individual letter frequencies in 4 million characters of English text [**2**, p. 4].



Letter	Frequency	Probability	Letter	Frequency	Probability
A	321712	.0804	N	283561	.0709
B	61472	.0154	O	303844	.0760
C	122403	.0306	P	79845	.0200
D	159726	.0399	Q	4226	.0011
E	500334	.1251	R	244867	.0612
F	92100	.0230	S	261470	.0654
G	78434	.0196	T	370072	.0925
H	219481	.0549	U	108516	.0271
I	290559	.0726	V	39504	.0099
J	6424	.0016	W	76673	.0192
K	26972	.0067	X	7779	.0019
L	165559	.0414	Y	69334	.0173
M	101339	.0253	Z	3794	.0009

Based on this, the plaintext of the ciphertext above is

(NUMBE R)(THEO RY)(HAS) (PLAYE D)(AN)(IM
PORTA NT)(ROL E)(IN)(TH E)(DEVE LOPME
NT)(OF)(C RYPTO SYSTE MS).

The level of security is increased by adding *substitution ciphers* and *polyalphabetic ciphers*. A substitution cipher is a cipher that replaces letters of the plain text with another set of letters or symbols while a polyalphabetic cipher is a system of substitution that mixes together a number of cipher alphabets in a cryptogram so that each plaintext letter is represented by a cipher that repeatedly changes. Polyalphabetic ciphers guarantees that a given plaintext letter will not always be represented by the same ciphertext letter. A word is used as the key, so to encipher a message one uses a sequence of letters and different generalized Caesar Ciphers at once. In 1975, Whitfield Diffie and Martin Hellman proposed the public-key cryptosystem which relies on discovery in computational complexity theory. Complexity theory primarily deals with the analysis and design of algorithms and especially with the number of computational steps needed to complete an algorithm [**2**, p. 7].

A *cryptosystem* consists of the algorithm for encryption and a piece of information, the key. In public-key cryptosystems each user has an encryption function and a decryption function. The encryption functions and the keys are made public to all users, but the decryption function is kept secret to only the owner. D and E are inverse transformations, that is, $E(D(C)) = C,$ and $D(E(P)) = P.$ The point is that the encryption/decryption functions are set up so that D is very difficult to compute only knowing $E.$ The *RSA* Public-Key Cryptosystem developed in 1977 by Ronald L Rivest, Adi Shamir and Leonard Adleman is the most secure ciphering algorithm. This algorithm involves intense mathematical structures and is based upon *Fermat's Little Theorem* with two large distinct prime numbers *p* and q. This cryptosystem is further investigated in the next chapter.

Chapter 3: The RSA Public Key and Cryptosystems

RSA, the trapdoor cipher certainly changed the face of cryptography in 1977. RSA, the public-key cryptosystem, is based upon factoring large integers. Fermat's Little Theorem, which states, if p is prime and a is a positive integer not divisible by $p,$ then

$$a^{p-1} \equiv 1 \ (mod\, p),$$

is the backbone of this cryptosystem. To generate the public and private keys, each user must select two large distinct prime numbers p and q each about 100 digits long (for added security). Let $r = pq.$ $\phi(r)$ is an arithmetic function that counts the number of positive integers less than or equal to r that are relatively prime to $r.$ Calculating $\phi(r)$ is proven to be difficult for large values or r, but *Euler's Theorem* states that

$$\phi(r) \ = \ (p-1)(q-1).$$

Thus by selecting the two primes p and q ,$\phi(r)$ is easily calculated. Furthermore, in order to ensure security, *r* needs to be hard to factor. The fewer factors a product has, the harder it is to find the factors. Choose $e \in \mathbb{Z}$ such that $3 < e < r,$ and e is relatively prime to $\phi(r).$ Since $\gcd\big(e, \phi(r)\big) = 1,$ e has a multiplicative inverse modulo $\phi(r),$ called $d \in \mathbb{Z}.$ The product $e \times d$ is relatively prime modulo $\phi(r).$ When the numbers have been chosen, e and r become the public key, while the private key consists of d, p and $q.$

In order for the cipher to work, the values of p must be less than r and relatively prime to $r.$ The value of 1 and $(r-1)$ cannot be used because 1 raised to any power is going to remain 1. To encrypt, simply raise each number corresponding to the character to the power of e modulo $r.$ To decrypt, simply raise each encrypted code to the power of

d modulo r. For example, using the mapping $[A—00, Z—25]$, let $p = 47$ and $q = 61$ be the two selected primes. Then

$$r = pq = 2867$$

$$\text{and } \phi(r) = (47 - 1)(61 - 1) = (46)(60) = 2760.$$

Select $e = 49$ then use the Euclidean Algorithm to verify that it is relatively prime to $\phi\ (r)$:

$$\phi(r) = 2760 = 56(49) + 16$$

$$49 = 3(16) + 1$$

$$16 = 16(1) + 0$$

Since 1 is the last nonzero remainder, $\varphi(r)$ and 49 are relatively prime. Given that, e x d must equal 1 $(mod\ 2760)$, it is known that

$$49 \times d = k \times 2760 + 1$$
$$or\ 1 = 49 \times d - k \times 2760$$

where $k \in \mathbb{Z}$. Using the Euclidean Algorithm in reverse:

$$1 = 49 - 3(16)$$

$$1 = 49 - 3(2760 - 56(49))$$

$$1 = 169(49) - 3(2740)$$

Therefore $d = 169$.

The resulting encryption algorithm is $E(P) = P^{49}\ (mod\ 2867)$, and the decryption algorithm is $D(C) = C^{169}(mod\ 2867)$ where P and C are numeric blocks less than 2867.

Substitution and *transposition* have been techniques for encryption since the birth of cryptography. Substitution is the simplest form of data confusion which is obscuring the relationship between plaintext and ciphertext. Transposition is the simplest form of diffusion which involves spreading the changes throughout the ciphertext. As mentioned in Chapter 2, frequency analysis is a strong tool against both techniques. Linear functions for encryption are not ideal since they can be broken by elementary algebra tactics of solving systems of equations. However, linear functions cover all of the requirements for efficient cryptosystems. They must be invertible, fast to compute, and should have small key size and memory requirements. To overcome the weakness of solely using linear functions, the integration of *XOR,* (Exclusive OR) a bitwise operator from binary mathematics, substitution, and permutation is introduced. The XOR operator is indicated by $\oplus$, which returns a 1 when the value of either the first bit **or** the second bit is a 1 and returns 0 when neither or both of the bits are 1. The XOR operator is used to flip bits (zeroes and ones) in a piece of plaintext to create a ciphertext. The combination or XOR, substitution and permutation results in an *iterative block cipher,* a cryptosystem that operates on a block of data and sequentially repeats a set of primitives. Each repetition is called a round. The *Data Encryption Standard* (DES), approved in 1977 by the National Bureau of Standards, is such a block cipher.

Horst Feistal, proposed a self-invertible design for block-structured cryptosystems. DES operates on a 64-bit data block using a 56-bit key. In order to encrypt a block of data, the block is split in half and the two 32-bit parts are operated on independently; right $R_{0,}$ and the left, L_0. In each round, the right half R_i becomes the new left half $L_{i+1.}$ The new right half is a function of the old right and left halves and a portion of the key K_{i+1} used in that round. Here f is the cipher function. That is,

$$L_i \leftarrow R_{i\text{-}1,}$$

$$R_i \leftarrow L_{i\text{-}1} \oplus f\,(R_{i\text{-}1,}\ K_i).$$

The cipher function, *f*, produces a 32-bit output data block from a 32-bit input data block

$R_{i\text{-}1}$ and $K_{i,}$ a 48-bit subkey. The function *f*, consists of an expansion *E,* bitwise addition, a substitution function *S,* an a permutation *P*.

$$f\,(R_{i\text{-}1,}\ K_i) = P(\ S(E(R_{i\text{-}1}) \oplus K_i))$$

The function *E* expands the 32-bits to 48-bits by splitting the data into eight 4-bit blocks and adding the least significant bit of one block to the end of the next block, then adding the most significant bit to the beginning of the proceeding block. The result of the expansion is then XORed to the 48-bit subkey K_i, producing the 48-bit input for *S*. *S* is the only nonlinear ingredient in the DES. There are eight S-boxes and each maps 6 bits to 4 bits in a 4 x 16 table. The output of each S-box is determined by the instruction bits and the data bits. The two outermost bits of the input are linked together to determine the row of the S-box, and the middle four bits determine the column of the S-box. The 4-bit integer at the row and column of the S-box is the output (substitution). Since each output is only 4-bits the result is a 32-bit block. *P* permutes the output from the S-boxes to cause diffusion and produces the output of the cipher function. This is then XORed with $L_{i\text{-}1}$ to determine the new right half. The algorithm to decrypt the data block is the same as the encryption, but the subkeys are applied in reverse order.

In order to make decryption a genuine inverse of encryption, the halves are switched in the final round of a Feistel cipher. Figure 1 shows the 16-round DES cipher which begins with an initial permutation, *P*, and ends with the inverse permutation,

P^{-1}.These permutations are not cryptographically important, but the DES is not complete without them. *S* is the substitution-box function (hereafter referred to as the *S*-box) used to obscure the relationship between the key and the ciphertext. The rounds are where the important mathematical cryptographic work occurs.

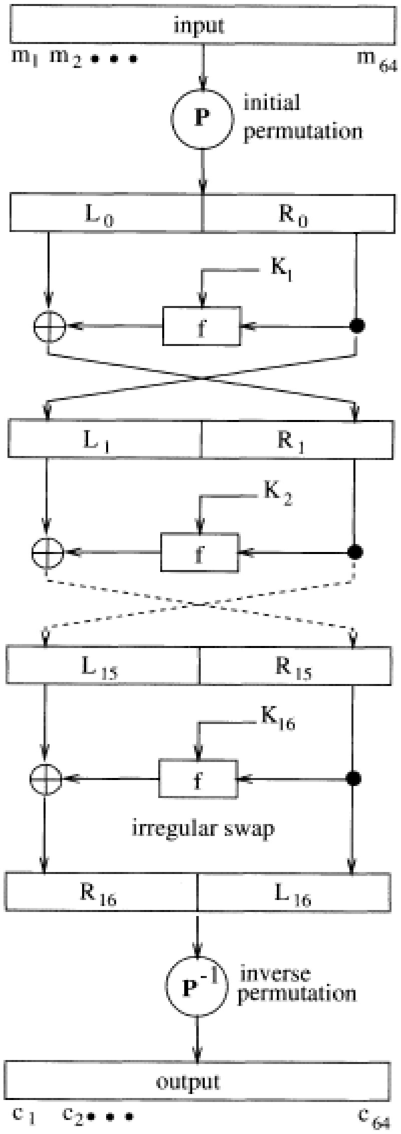


Figure 1. Data Encryption Standard [**7**, p 93]

The DES algorithm was the Federal Standard from 1977-the early 2000s when it was replaced by the Advance Encryption Standard. Cryptography represents are only a small spectra of algorithms, different examples are examined in the subsequent chapter.

Chapter 4: A New Version of the Euclidean Algorithm

The Euclidean Algorithm is a method used to find the greatest common divisor of two positive integers, a and b. The algorithm is based on two observations. First, if b divides a, then the $gcd(a,b) = b.$ The second observation provides the basis for the Euclidean Algorithm. If $a = bq + r,$ for integers q and r, then $gcd(a,b) = gcd(b,r)$. Using the division algorithm repeatedly results in

$$a = bq_1 + r_1 \, with \, 0 \leq r_1 < b,$$

$$b = r_1q_2 + r_2 \, with \, 0 \leq r_2 < r_1,$$

and so on. Since $r_1 > r_2 > \cdots r_n,$ the remainders are decreasing. In finitely many steps a remainder of

$$r_n = 0$$

is obtained. Thus,

$$gcd(a,b) = gcd(b,r) = \cdots = r_{n-1}.$$

There is a very important corollary consequence which follows from the algorithm. If a and b are nonzero integers, their GCD is a linear combination of a and b, that is there are two integers s and t such that

$$as + bt = gcd(a,b).$$

Blankinship offers an alternative matrix algorithm which, although equivalent to the Euclidean Algorithm, is much easier to visualize and be programmed on paper or on a computer [**1**, p. 742]. Using the algorithm, given a set of positive integers $a_1, a_2, \ldots\, a_n,$

one can compute the greatest common divisor, d, of these numbers. It is also possible to deduce elements $x_1, x_2, \ldots\ x_n$such that

$$d = a_1x_1 + a_2x_2 + \cdots + a_nx_n.$$

This again, is the results of the corollary.

The algorithm is computed by preparing a $n \times (n+1)$ matrix, and performing elementary row operations in order to reduce all but one of the elements in the first column to zero. The first element in each row is referred to as the leader element. The matrix used consists of positive integers $a_1, a_2, \ldots\ a_n$ in the first column, and the appropriate sized identity matrix affixed as shown in Figure 2:

$$\begin{array}{cccccccc}
a_1 & 1 & 0 & 0 & . & . & . & 0 \\
a_2 & 0 & 1 & 0 & . & . & . & 0 \\
a_3 & 0 & 0 & 1 & . & . & . & 0 \\
. & . & . & . & . & . & . & . \\
. & . & . & . & . & . & . & . \\
. & . & . & . & . & . & . & . \\
a_\mathrm{n} & 0 & 0 & 0 & 0 & . & . & 1
\end{array}$$

Figure 2. Algorithm Matrix Setup [**1**, p. 742]

After completion of five steps of elementary row operations, there is only one row with a nonzero leader. The remaining row is

$$d, x_1, x_2, \ldots\ x_n$$

where d is the greatest common divisor of $a_1, a_2, \ldots a_n$. By the corollary, d can be written as a linear combination of the positive integers. That is

$$d = a_1x_1 + a_2x_2 + \cdots + a_nx_n.$$

Blankinship describes the five steps used to eliminate leader elements, and verifies that the process terminates by noting that every fourth step, a column leader decreases but will never be negative. Step 1: Select the row with the smallest nonzero leader and call it the "operator." Step 2: Select any other row with a nonzero leader and call it the "operand." (When no operand can be found the process is completed.) Step 3: Divide the leader of the operator into the leader of the operand, ignoring the remainder. Denote the quotient by q. Step 4: Subtract q times the operator from the operand, recording the result as a new row and striking out the operand. Step 5: Return to step 1 [**1**]. It is essential that it is noted that the greatest common divisor is preserved through the row operations. That is

$$\text{gcd}\,(b_1, b_2, \ldots b_n) = gcd(b_1 + ab_j, b_2, b_3, \ldots, b_n)$$

for any integer a and any $j \le n$ different from 1. When the last step is reached all the leaders are zero except that of the previous operand and that number must be the GCD of the original leaders.

Blankinship provides an example with three positive integers $a_1 = 99, a_2 = 77,$ and $a_3 = 63$.

99	1	0	0
77	0	1	0
63	0	0	1

After repetitive row reduction and elimination, the remaining row with a nonzero leader is

$$1 \qquad 1 \qquad 56 \qquad -70$$

which is interpreted to mean

$$1 = 1 \text{ x } 99 + 56 \text{ x } 77 - 70 \text{ x } 63.$$

Using this matrix algorithm the greatest common divisor is determined to be 1, and it is shown that it can be written as a linear combination of positive integers $a_1, a_2,$ and a_3. This resulting equation lends effortlessly to the *Chinese Remainder Theorem* which determines a number m such that m is a unique solution to simultaneous linear congruences modulo p. The Chinese Remainder Theorem is applicable only when $d = 1$, that is, the integers are relatively prime. The resulting equation from the example above can be simplified by reducing all of the columns by the appropriate prime. Then,

$$1 = 1 \text{ x } 99 + 2 \text{ x } 77 + 7 \text{ x } 63 \ (mod\ 693)$$

Or,

$$m = 99m_1 + 154m_2 + 441m_3 \ (mod\ 693).$$

Substitution for $m_1, m_2,$ and m_3, produces the smallest number m which satisfies simultaneous linear congruences. A Euclidean ring is a ring without zero divisors in which an integer norm and an associated division algorithm can be defined. This algorithm is applicable to any Euclidean ring, as long as the elements of smaller and larger are interpreted according to the ring's norm. Blankinship elaborates on how this method can be rephrased for polynomials over a field. In this case, coefficients are referred to as the lead elements, and are reduced according to degree.

The alternative to the Euclidean Algorithm has two major advantages. This method offers the ease of computer programming, as well a simplified organization structure for the computational work. Reduction of integers is done using modular arithmetic. Modular arithmetic can be used to obtain information about the solutions (or lack thereof) of any specific equation. The study of Gaussian Integers and modular arithmetic is investigated in the next chapter.

Chapter 5: Exploring Gaussian Integers

This chapter explores the extensions of common properties of the integers to the Gaussian Integers. One defines the set of Gaussian Integers as

$$\mathbb{Z}[i] = \{a + bi|a, b \ \in \mathbb{Z}\}$$

where $\mathbb{Z}$ denotes the set of ordinary integers. It is common knowledge that for $a \ \in \mathbb{Z}$, $|a|$ represents the size of a. The magnitude of a Gaussian Integer $\alpha = a + bi \in \mathbb{Z}[i]$ is determined by the norm defined as $N(\alpha) = a^2 + b^2$. In $\mathbb{Z}$, size is measured by the absolute value. In $\mathbb{Z}[i]$ we use the norm.

$$N(\alpha) = \alpha\bar{\alpha} = (a + bi)(a - bi) = a^2 + b^2$$

$$N(\alpha\beta) = N(\alpha) \times N(\beta).$$

Thinking about $a + bi$ as a complex number, its norm is the square of its usual absolute value:

$$|a + bi| = \sqrt{a^2 + b^2}$$

$$N(a + bi) = a^2 + b^2 = |a + bi|^2$$

The reason we prefer to deal with norms on ℤ[i] instead of absolute values on ℤ[i] is that norms are integers (rather than square roots), and the divisibility properties of norms in ℤ will provide important information about divisibility properties in ℤ[i].

In this ring we define two terms. A *unit* is any element which has a multiplicative inverse. *Associates* are elements which differ by a unit factor- e.g. , if u is a unit and

$a = bu$, then a and b are associates. There are four units in $\mathbb{Z}[i]$; $\pm 1,\ \pm i$. This is shown by using the property:

$$N(\alpha\alpha^{-1}) = N(\alpha)N(\alpha^{-1}) = N(1) = 1.$$

Therefore,

$$N(\alpha) = N(\alpha^{-1}) = 1.$$

Primes in $\mathbb{Z}[i]$ are non-zero elements which are not units and cannot be factored without using a unit. In other words, analogous to $\mathbb{Z}$, primes in $\mathbb{Z}[i]$ have only two factors, itself or an associate and a unit. For example, α is prime if $\alpha = \beta\gamma \rightarrow$ just one of β or γ is a unit. To determine which elements in $\mathbb{Z}[i]$ are primes, one considers the elements, other than 0 and units, with the smallest norm. Let

$$\alpha = (1 + i)$$

since

$$\alpha = \beta\gamma,$$

then

$$2 = N(\alpha) = N(\beta\gamma) = N(\beta)N(\gamma)$$

so either β or γ are units and therefore α is prime. In general, if $N(\alpha)$is prime in $\mathbb{Z}$ then α is prime in $\mathbb{Z}[i]$. The only primes in $\mathbb{Z}[i]$ are $\pm(1 + i)$ and $\pm(1 - i)$. In Figure 3 the multiples of $(1 + i)$ are represented by dots, which are obviously all composite, and those which are primes are represented by squares. Note that there is a geometric pattern.

In $\mathbb{Z}$, there is a method called the Sieve of Eratosthenes used for finding a list of prime numbers, see Figure 4. Beginning by circling the smallest prime integer and crossing out all of its multiples, then circling the next smallest integer, and crossing out all of its multiples, and continuing the process one can discover a subset of prime integers.

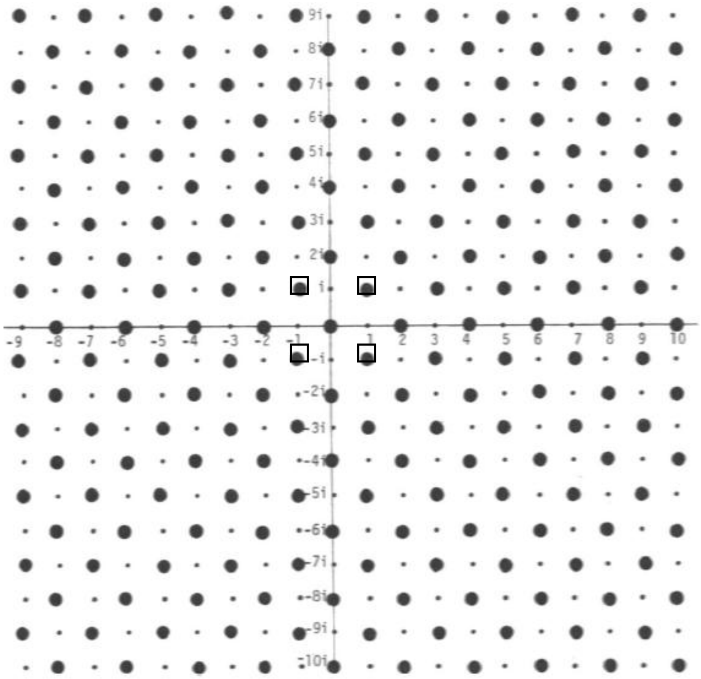
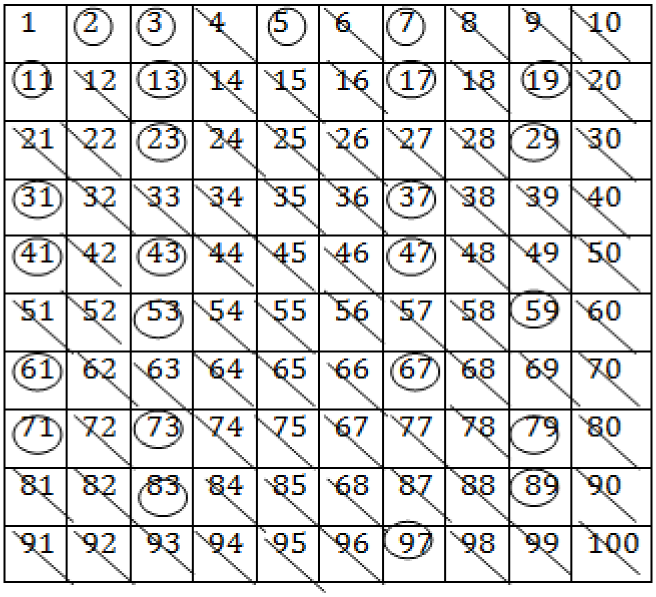


Figure 3. Multiples of $(1 + i)$ [**1**, p. 6]

Table 3. Sieve of Eratosthenes in $\mathbb{Z}$



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~~	~~67~~	~~77~~	~~78~~	79	~~80~~
~~81~~	~~82~~	83	~~84~~	~~85~~	~~68~~	~~87~~	~~88~~	89	~~90~~
~~91~~	~~92~~	~~93~~	~~94~~	~~95~~	~~96~~	97	~~98~~	~~99~~	~~100~~

A similar method can be used in $\mathbb{Z}[i]$. Figure 4 shows the result of applying the sieve in $\mathbb{Z}[i]$ up to norm 53. Notice that some numbers are prime in $\mathbb{Z}$ but are not prime in $\mathbb{Z}[i]$. This follows directly from the factorizations. A prime p in $\mathbb{Z}$ is composite in $\mathbb{Z}[i]$ if and only if it is a sum of two squares. Thus, any prime p in $\mathbb{Z}$ which is not a sum of two squares is not composite in $\mathbb{Z}[i]$, so it stays prime in $\mathbb{Z}[i]$. In general, if p is prime in $\mathbb{Z}$, but not prime in $\mathbb{Z}[i]$, then

$$|p| = (a + bi)(a - bi),$$

so

$$|p| = a^2 + b^2$$

For example, primes $2, 5, 13, 17, 29$ ... are equal to the sum of two squares, and can also be written in the for $|p| = 4k + 1$. In fact, one can show that every rational prime in the form $4k + 1$ is prime in $\mathbb{Z}$ but composite in $\mathbb{Z}$[i].

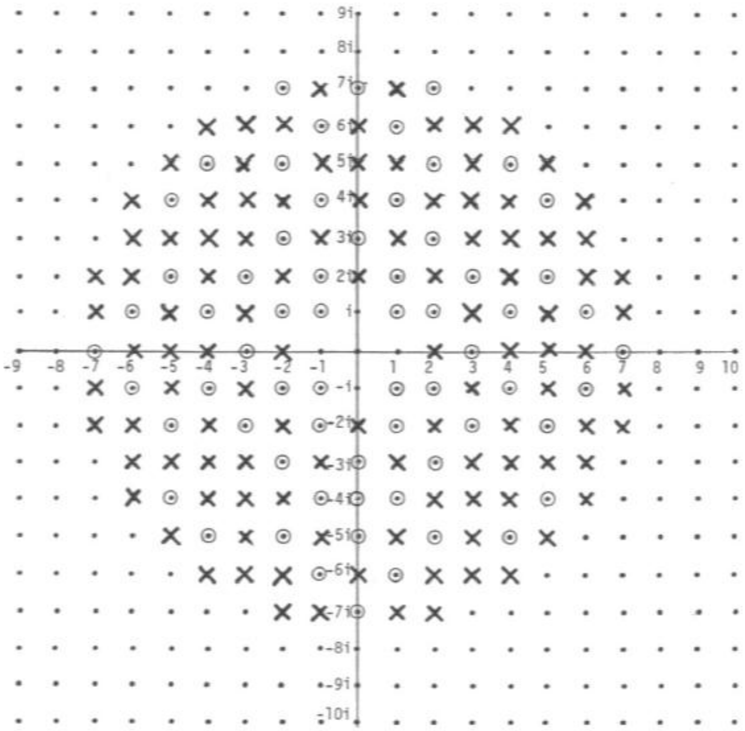


Figure 4. Geometric Model [**6**, p. 7]

Residue classes and congruences from modular arithmetic have been defined and applied in ℤ[i]. $\forall\, \alpha, \beta, \gamma \in \mathbb{Z}[i]$, $\alpha \equiv \beta (mod\, \gamma)$ if $\alpha - \beta$ is a mulitple of γ. $\beta(mod\, \gamma)$ is defined as $\{\alpha | \alpha \in \mathbb{Z}[i]$ and $\alpha \equiv \beta(mod\, \gamma)\}$. When plotted, residue classes are translations of the multiples. Figure 4 shows an example of this geometric pattern. For instance, the residue class of $1 + i(mod\ 2 + i)$ is denoted by stars while the multiples of $2 + i$ are denoted by dots. In order to determine the number of residue class that exist for a particular element, one must compute the norm. In general, there are $N\gamma$ residue classes modulo γ in $\mathbb{Z}[i]$, which is analogous to the fact that there are $|n|$ residue classes modulo n in ℤ.

If p is prime and $\alpha \not\equiv 0(mod\, p)$, then, by Fermat's Little Theorem, $\alpha^{p-1} \equiv 1(mod\, p)$. This theorem holds in $\mathbb{Z}[i]$ as well. That is, if π is prime in $\mathbb{Z}[i]$, and α is not a mulitple, then $\alpha^{N\pi-1} \equiv 1(\text{mod}\, \pi)$. Fermat's Theorem in $\mathbb{Z}$ can be generalized to Euler's Theorem that if $gcd(a, n) = 1$, then $a^{\phi n} \equiv 1\, (mod\, n)$. $\phi(n)$ is Euler's phi function. As long as two elements being relatively prime is defined in $\mathbb{Z}[i]$, then by transitivity one can say that

$$\phi(\pi) = N\pi - 1.$$

$\phi(\pi)$ denotes the number of units in the ring $\mathbb{Z}[i]/\pi$.

There are many theorems in the field of number theory which have analogies from $\mathbb{Z}$ to $\mathbb{Z}$[i]. The Chinese Remainder Theorem and Fermat's Last Theorem, are just a few. In order to prove the analogy in the $\mathbb{Z}[\sqrt{-3}]$, one faces the challenge of restoring the uniqueness of prime factorization. In $\mathbb{Z}[i]$ and $\mathbb{Z}[\sqrt{-2}]$ prime factorization holds uniqueness, however in $\mathbb{Z}[\sqrt{-3}]$ one must enlarge the set of integers to include all those of the form $a + b\sqrt{-3}$ where a and b are both in $\mathbb{Z}$ and both halves of odd integers in $\mathbb{Z}$.

Chapter 6: Conclusion

Algorithmic number theory is an expansive area of study in modern mathematics and is normally studied in a post secondary setting. In the standard secondary mathematics structure and sequence, algorithmic number theory is not formally introduced. However, some of the topics of study in high school algebra and geometry are underlying basics of more complex algorithms. It is important that teachers emphasize to students that many topics in math are cross disciplinary areas of study. Liberal arts are rarely ever linked to mathematics in the classroom. However, the study and use of cryptography plays an important role in world history as well as linguistics (language arts). In World War 2, the Allied forces utilized it to break the Purple Code of Japan which lead to strategic movements in the Pacific. One of the world's most acclaimed poets, Edgar Allen Poe, fancied himself as a cryptanalyst [**2**, p. 2].

In order to effectively encourage depth and complexity of understanding, it is important to bring together different topics of mathematics and show students how they are related. The National Council of Teachers in Mathematics suggests that students "recognize and use connections among mathematical ideas" [**4**, p. 1]. In algebra, students could be introduced to the matrix method of solving systems of equations, as well as for factoring equations. Following matrix instruction, students can use matrix techniques on various types of mathematics problems, in order to make connections and use algebraic symbols to represent various solutions. Connections between the various concepts will certainly broaden the understanding of each topic and thus increase students' appreciation for the beauty of mathematics and numerical interactions.

Reference

1. Blankinship, W. A. "A New Version of the Euclidean Algorithm." *The American Mathematical Monthly*, Vol. 70, No. 7 (1963): 742-745.

2. Dennis Luciano, Gordon Prichett “Cryptology: From Caesar Ciphers to Public-Key Cryptosystems.” *The College Mathematics Journal*, Vol. 18, No. 1 (Jan., 1987): 2-17

3. Paulo Ribenboim "Are There Functions That Generate Prime Number?" *The College Mathematics Journal*, Vol. 28, No. 5 (Nov., 1997): 352-359.

4. Principles and Standards for School Mathematics. 2000. Retrieved November 23, 2012; available at http://standards.nctm.org/.

5. Pythagorean Triples. Retrieved March 12, 2013; available at http://www.math.brown.edu/~jhs/frintch1ch6.pdf.

6. Robert G. Stein "Exploring Gaussian Integers.” *The College Mathematics Journal*, Vol. 7, No. 4 (Dec., 1976): 4-10

7. Susan Landau, “Polynomials in the Nation’s Service: Using Algebra to Design the Advance Encryption Standard.” *The American Mathematical Monthly*, Vol. 111, No. 2 (Feb., 2004): 89-117

Vita

Upon graduation from Wharton High School in Wharton, Texas, Ariel Jolishia Taylor moved to Austin, Texas to attend the University of Texas in 2007. There she earned her BS in Mathematics, completed the UTeach Program, and received her Business Foundations Certificate in May 2011. She taught Algebra 2 and Geometry courses at Mary Carroll High School in Corpus Christi, Texas during her first year of teaching. Currently, she teaches Algebra 1 at Lyndon B. Johnson High School in Austin, Texas. In the summer of 2011, she entered the Graduate School at The University of Texas at Austin pursing a MA in Mathematics.

Email Address: arieltaylor@utexas.edu

This report was typed by Ariel Jolishia Taylor