Coding through the perspective of Fermat Theorem and Residue System

T. Srinivasa Rao, Asst. Prof., UCST, AKNU, tsr.math@aknu.edu.in

Abstract: the Little Fermat theorem helps us to define congruence relation using the relatively primeness. Further divisibility rules help to create the highest powers of primes confirm the residues. This in turn helps to create Cartesian coordinate system of residues while any number *n* can have at most $\varphi(n)$ distinct residues. Using this residue system as the Cartesian coordinates, we can create concatenated strings formed from the ordered $\varphi(n)$- tuple that follow all the properties of a commutative ring. If the system is created using the composite numbers, then there will be zero divisors and otherwise, the commutative ring will be a field under usual addition and usual multiplication at the powers of the primes. These $\varphi(n) -$ tuples can be encoded using the technique of cross product of $\varphi(n)$ – length and decoded using the reverse cross product technique.

1. **Introduction**:

A prime number is relatively prime to every other number except to its multiples. So, if *p* is prime and (*a*, *p*) = 1 with $a \neq 1$, then it follows a is not a multiple of *p*. so, Little Fermat theorem says "$a^{p-1} \equiv 1 mod p$ whenever *p* is prime and gcd (*a, p*) = 1"
A prime number is relatively prime to every number except to its multiples.
Taking *p* = 1531, *a* = 6, we have $6^{1530} \equiv 1 mod 1531$

If $a \equiv b \ mod \ m; c \equiv d \ mod \ m$, then $m|a - b, m|c - d$
Also, $m|ac - bc, m|bc - bd$
So, $m|(ac - bc) + (bc - bd)$
This helps $ac \equiv bd \ mod \ m$
Using this, $a^n \equiv b^n mod \ m$ for every positive integer *n* and whenever $a \equiv b \ mod$.

We can construct codes of length $\varphi(n)$ for each number *n* such that the residues of each location of the *n* – length Cartesian coordinates or concatenated string will replace the actual number present in the location where $\varphi(n)$ is the Euler totient function.

2. **Creating a code using φ(n):**

For instance, $\varphi(32) = 14$
We can write 14 length code (1000, 12, 28, 39, 57, 643, 51225, 2123, 5152, 999, 1, 123, 13, 29)
$a^n \equiv b_i mod \ m, 1 \leq i \leq k$ and $s \equiv t \ mod \ k$, then $a^s = {b_i}^t mod \ m$ …… 2.1

See that $4^4 \equiv 4 \ \ mod \ 14; 4^8 = (4^4)^2 = 4^2 \ \ mod \ 14 \equiv 2 \ mod \ 14$
$(4^4)^3 \equiv 2^3 mod \ 14$ or simply $4^{12} \equiv 8 \ \ mod \ 14$; $4^{16} \equiv (4^8)^2 \equiv 2^2 = 4 \ \ mod \ 14$;
$4^{20} = (4^4)^5 \equiv 4^5 = 4^4 \times 4 = 4 \times 4 \equiv 2 \ \ mod \ 14$; $4^{24} \equiv 8 \ \ mod \ 14$; …
It is observed that
$4^4 \equiv 4^{16} \equiv 4^{28} \equiv 4^{40} \equiv \cdots \equiv 4 mod \ 14$
$4^8 \equiv 4^{20} \equiv 4^{32} \equiv 4^{44} \equiv \cdots \equiv 2 mod \ 14$
$4^{12} \equiv 4^{24} \equiv 4^{36} \equiv 4^{48} \equiv \cdots \equiv 8 mod \ 14$

https://doi.org/10.5281/zenodo.17347188

The generalization is
$4^{3n+1} \equiv 4 \; mod \; 14,$ ...... (i)
$4^{3n+2} \equiv 2 \; mod \; 14$ ...... (ii)
$4^{3n} \equiv 8 \, mod \; 14$ ...... (iii)
In view of this discussion,
$32^{1000} = (28+4)^{1000} \equiv 4^{1000} mod \; 14$
Note that every other term of this expansion is a multiple of 28 which is congruent to 0 mod 14.
$\equiv 4^{3(333)+1} \equiv 4 \; mod \; 14$ by (i).
Using the above discussion, $32^{1000} \equiv 4 \, mod \; 14$ 1
$32^{12} \equiv (28+4)^{12} mod \; 14 \equiv 4^{12} \equiv 4^{3(4)} mod \; 14 \equiv 8 \, mod \; 4$ 2
$32^{28} mod \; 14 \equiv 4^{28} mod \; 14 \equiv 4^{3(9)+1} \; mod \; 14 \equiv 4 \, mod \; 14$ 3
$32^{39} mod \; 14 \equiv 4^{39} mod \; 14 \equiv 4^{3(13)} \equiv 8 \, mod \; 14$ 4
$32^{57} mod \; 14 \equiv 4^{57} mod \; 14 \equiv 4^{3(19)} \equiv 8 \, mod \; 14$ 5
$32^{643} mod \; 14 \equiv 4^{643} mod \; 14 \equiv 4^{3(214)+1} \; mod \; 14 \equiv 4 \, mod \; 14$ 6
$32^{51225} mod \; 14 \equiv 4^{51225} mod \; 14 \equiv 4^{3(17075)} mod \; 14 \equiv 8 \, mod \; 14$ 7
$32^{2123} mod \; 14 \equiv 4^{2123} mod \; 14 \equiv 4^{3(707)+2} \; mod \; 14 \equiv 2 \, mod \; 14$ 8
$32^{5152} mod \; 14 \equiv 4^{5152} mod \; 14 \equiv 4^{3(1717)+1} \; mod \; 14 \equiv 4 \, mod \; 14$ 9
$32^{999} mod \; 14 \equiv 4^{999} mod \; 14 \equiv 4^{3(333)} \; mod \; 14 \equiv 8 \, mod \; 14$ 10
$32^{1} mod \; 14 \equiv 4^{1} mod \; 14 \equiv 4 \, mod \; 14$ 11
$32^{123} mod \; 14 \equiv 4^{123} mod \; 14 \equiv 4^{3(41)} \; mod \; 14 \equiv 8 \, mod \; 14$ 12
$32^{13} mod \; 14 \equiv 4^{13} mod \; 14 \equiv 4^{3(4)+1} \; mod \; 14 \equiv 8 \, mod \; 14$ 13
$32^{29} mod \; 14 \equiv 4^{29} mod \; 14 \equiv 4^{3(9)+2} \; mod \; 14 \equiv 2 \, mod \; 14$ 14

So, the code congruent modulo 14 to
(1000, 12, 28, 39, 57, 643, 51225, 2123, 5152, 999, 1, 123, 13, 29) is
(4, 8, 4, 8, 8, 4, 8, 2, 4, 8, 4, 8, 8, 2)
Note that each code in $\mathbb{Z} \times \mathbb{Z} \times ... \times \mathbb{Z}_{\varphi(n)}$ has a unique code of length $\varphi(n)$- tuple residue modulo *n*, but each code residue modulo *n* is not necessarily assigned to a unique code in $(\mathbb{Z} \times \mathbb{Z} \times ... \times \mathbb{Z})_{\varphi(n)}$.

Addition of $\varphi(n)$ length Cartesian codes obeys closure law under addition as well as multiplication.

Consider a plain text for the residues of $\varphi(32)$ as
A=(5,6,7,8,9,10,11,12,13,1,2,3,4,5) = 567891011121312345 ...... 2.2
Since *n* = 14 which is of two digited number, each character in the string will be identified with two digit locations. So, *A* can be written as 0506070809101112130102030405
B=(2,2,2,3,4,10,3,5,4,10,11,12,13,13)
= 0202020304100305041011121313 ...... 2.3
C=(5,10,10,2,3,6,7,3,3,4,5,6,7,8)
= 0510101020306070303040506070 8 ...... 2.4

A+*B* = (7,8,9,11,13,20,14,17,17,11,13,15,17,18)
(*A*+*B*)*C*= (5*7, 10*8, 10*9, 2*11, 3*13, 6*20, 7*14, 3*17, 3*17, 4*11, 5*13, 6*15, 7*17,8*18)

$(A+B)C$= (35,80,90,22,39,120,98,51,51,44,65,90,119, 144) …… 2.5
= (2, 2, 0, 1, 0, 0, 2, 0 , 0, 2, 2, 0, 1, 0)
AC = (25, 60, 70, 16, 27, 60, 77, 36, 39, 4, 10, 18, 28, 40)
= (1, 0, 1, 1, 0, 0, 2, 0, 0, 1, 1, 0, 1, 1)
BC = (10, 20, 20, 6, 12, 60, 21, 15, 12, 40, 55, 72, 91,104)
= (1, 2, 2, 0, 0, 0, 0, 0, 0, 1, 1, 0, 0, 2)

$AC + BC$ = (2, 2, 0, 1, 0, 0, 2, 0, 0, 2, 2, 0, 1, 0) …… 2.6
(2.5) and (2.6) confirm that distributivity of the powers of primes using addition over multiplication obeys the residue system. …… 2.7

3. Encryption of a string of residues:

$(\mathbb{Z} \times \mathbb{Z} \times \ldots \times \mathbb{Z})_{\varphi(n)}$ is the Cartesian product of residue class rings such that at least one n_i, $1 \leq i \leq k$ is a composite number.
From (2.1), it is seen that $\varphi(32) = 14$. So, considering the 14 distinct powers of 32 as strings of length 14, the strings in (2.2) through (2.6) are formed. These strings can further be encrypted and decrypted as follows.

Using the technique of cross product system on the $\varphi(n)$ length code, the resulting determinant model can be seen in the following way.

Considering $d_1 d_2 \ldots d_{\varphi(32)}$ as the encryption key, the plain text having the code $e_1 e_2 \ldots e_{\varphi(32)}$ will be enciphered as follows. …… 2.8

N_1	N_2	N_3	N_4	N_5	N_6	N_7	N_8
d_2 d_3	d_3 d_4	d_4 d_5	d_5 d_6	d_6 d_7	d_7 d_8	d_8 d_9	d_9 d_{10}
e_2 e_3	e_3 e_4	e_4 e_5	e_5 e_6	e_6 e_7	e_7 e_8	e_8 e_9	e_9 e_{10}

N_9	N_{10}	N_{11}	N_{12}	N_{13}	N_{14}
d_{10} d_{11}	d_{11} d_{12}	d_{12} d_{13}	d_{13} d_{14}	d_{14} d_1	d_1 d_2
e_{10} e_{11}	e_{11} e_{12}	e_{12} e_{13}	e_{13} e_{14}	e_{14} e_1	e_1 e_2

…… 3.1

Assume that A is the encryption key given in (2.2) and the code in (2.3) is to be encrypted.
It can be done as

N_1	N_2	N_3	N_4	N_5	N_6	N_7	N_8	N_9	N_{10}
6 7	7 8	8 9	9 10	10 11	11 12	12 13	13 1	1 2	2 3
2 2	2 3	3 4	4 10	10 3	3 5	5 4	4 10	10 11	11 12

N_{11}	N_{12}	N_{13}	N_{14}
3 4	4 5	5 5	5 6
12 13	13 13	13 2	2 2

…… 3.2

Note that the highest term possible in $N_i -$ location will be $14 \times 14 - 0 = 196$ which is a 3 digit number and so is, each location of the enciphered code would occupy 3 digit string.
On simplification, the required code using modulus is

N_1	N_2	N_3	N_4	N_5	N_6	N_7	N_8	N_9	N_{10}
-2	5	5	50	-80	19	-17	126	-11	-9

N_{11}	N_{12}	N_{13}	N_{14}
-9	-13	-55	-2

…… 3.3

Applying modulo 14, this becomes

N_1	N_2	N_3	N_4	N_5	N_6	N_7	N_8	N_9	N_{10}
12	9	9	8	4	5	11	0	3	5

N_{11}	N_{12}	N_{13}	N_{14}
5	1	1	12

…… 3.4

The encrypted code has $3\varphi(n)$ length in which if the calculation in (3.3) bears negative sign, then the code in the respective i^{th} - place will be 1 and otherwise 0, $\varphi(n) + 1 \leq i \leq 2\varphi(n)$.
Also, the entry in the $j^{th} -$ location will be number of times the division conducted.
When *n* has two decimal digits, then each location in the cipher text will be
012 009 009 008 004 005 011 000 003 005 005 001 001 012 10001010111101 01 01 03 06 01 02 09 01 01 01 01 04 01 …… 3.5
This is the required cipher text.

4. Decryption of the Cipher Text:

The decryption process will consider 3 digit string starting from left for $3n$ digits, considers the residue initially bears negative sign if 1 is the location between $3n + 1$ to $4n$ and two location string from $4n + 1$ to $6n$ locations that the number of times the modular operation is performed.

012	009	009	008	004	005	011	000	003	005
005	001	001	012						

It is nothing but $12, 9, 9, 8, 4, 5, 11, 0, 5, 5, 5, 1, 2, 12$ …… 4.2

10001010111110 which is equivalent to

-	+	+	+	-	+	-	+	-	-	-	-	-	-

…… 4.3

That means, the residue is negative in the 1st location, 2nd is positive and so on.
12 – 14 = - 2, 14 – 9 = 5, 14 – 9 = 5, 14 – 8 = 6, 4 – 14 = - 10, 14 – 5 = 9, 11-14= - 3, 14 – 0 = 0
5 – 14 = - 9, 5 – 14 = - 9, 5 – 14 = - 9, 13 – 14 = - 1, 12 -14= -2, 14 – 12 = 2

So, the string that suits $-2, 5, 5, 6, -10, 9, -3, 0, -9, -9, -9, -1, -2, 2$ …… 4.4
Let us take the encrypted string (3.5) from the location $4\varphi(32)+1$ to $6\varphi(32)$ and each substring of two characters are to be multiplied with the integer (4.4)
01,01,01,03,06,01,02,09,01,01,01,01,04,01 are to be multiplied with mod 14 and the following equations. …… 4.5
That is,
$d_2e_3 - d_3e_2 = -2$; $d_3e_4 - d_4e_3 = 5$; $d_4e_5 - d_5e_4 = 5$; $d_5e_6 - d_6e_5 = 6$;
$d_6e_7 - d_7e_6 = -7$; $d_7e_8 - d_8e_7 = 9$; $d_8e_9 - d_9e_8 = -3$; $d_9e_{10} - d_{10}e_9 = 0$;
$d_{10}e_{11} - d_{11}e_{10} = -9$;$d_{11}e_{12} - d_{12}e_{11} = -9$; $d_{12}e_{13} - d_{13}e_{12} = -9$; $d_{13}e_{14} - d_{14}e_{13} = -1$;
$d_{14}e_1 - d_1e_{14} = -2$; $d_1e_2 - d_2e_1 = 2$;

Using the encryption key (2.8), $d_1d_2 \dots d_{\varphi(32)} = 567891011121312345$ and (3.2) gives

$6e_3 - 7e_2 = -2$; $7e_4 - 8e_3 = 5$; $8e_5 - 9e_4 = 5$; $9e_6 - 10e_5 = 6$; $10e_7 - 11e_6 = -7$
$11e_8 - 12e_7 = 9$; $12e_9 - 13e_8 = -3$; $13e_{10} - 1e_9 = 0$; $1e_{11} - 2e_{10} = -9$
$2e_{12} - 3e_{11} = -9$; $3e_{13} - 4e_{12} = -9$; $4e_{14} - 5e_{13} = -1$; $5e_1 - 6e_{14} = 2$; $5e_2 - 6e_1 = 2$

After performing (4.5), these equations become
$6e_3 - 7e_2 = -1(14) + 12$; $7e_4 - 8e_3 = 5(1) = 5$; $8e_5 - 9e_4 = 5(1) = 5$;
$9e_6 - 10e_5 = 3(14) + (14 - 6)$; $10e_7 - 11e_6 = -6(14) + 4$
$11e_8 - 12e_7 = 2(14) - 9$; $12e_9 - 13e_8 = -2(14) + 11$; $13e_{10} - 1e_9 = 9(14) + 0$;
$1e_{11} - 2e_{10} = -1(14) + 3$; $2e_{12} - 3e_{11} = -1(14) + 5$; $3e_{13} - 4e_{12} = -1(14) + 5$; $4e_{14} - 5e_{13} = -1(14) + 1$; $5e_1 - 6e_{14} = -4(14) + 1$; $5e_2 - 6e_1 = -1(14) + 12$ …… 4.6

Substituting each of these equations in the immediate preceding and succeeding equations, each of values of $e_i, 1 \le i \le 14$ are obtained and so, the decrypted code is

$e_1e_2 \dots e_{\varphi(32)} = 22234103541011121313$ …… 4.7

The encryption key and system of non homogeneous equations will give the values of
$e_1, e_2, \dots, e_{\varphi(32)}$ that are nothing but the decrypted code.

It can be easily seen that $\varphi(635) = 52$ which is twice the number of alphabet. So, for coding lower and upper case alphabet, a code length of 52 and the powers of 635 can be considered for the above encryption and decryption procedure. Similarly, $\varphi(192) = 64$ that deal with all types of characters and numbers upon the keyboard for encryption.

References:

1. https://books.google.co.in/books?hl=en&lr=&id=hyO3CgAAQBAJ&oi=fnd&pg=PR7&dq=algebraic+coding+theory+and+applications&ots=aBoymPiWlM&sig=6QJV0ihgVEO7h96WcSrIqXVWKJc&redir_esc=y#v=onepage&q=algebraic%20coding%20theory%20and%20applications&f=false , Chapter 3.

2. https://www.google.co.in/books/edition/Fermat_s_Last_Theorem/ae5V08nnE8wC?hl=en&gbpv=1&dq=algebraic+coding+theory+and+applications+and+Fermat&pg=PA1&printsec=frontcover, Page 45

3. Fermat's Last Theorem and the Origin and Nature of the Theory of Algebraic Numbers; https://www.jstor.org/stable/2007234?origin=crossref&seq=1

4. https://www.tandfonline.com/doi/abs/10.1080/00029890.1918.11998451
Fermat Infinite Descent

5. https://doi.org/10.1201/9781439894699
https://www.taylorfrancis.com/books/mono/10.1201/9781439894699/applied-algebra-darel-hardy-fred-richman-carol-walker ; Codes, Ciphers, Discrete Algorithms – 2nd ed.

6. https://www.google.co.in/books/edition/Number_Theory/qEwpwWyVPIAC?hl=en&gbpv=1&dq=algebraic+coding+theory+and+applications+and+Fermat&pg=PR13&printsec=frontcover ; Quadratic Residues

https://doi.org/10.5281/zenodo.17347188