"Science Stays True Here"
Journal of Mathematics and Statistical Science (ISSN 2411-2518, USA), Vol.6, Issue 11, 310-320 | Science Signpost Publishing

Coprime Integer Encryption Algorithm Upon Euler's Totient Function's Unsolved Problems

Remzi Aktay

Kecioren Sehit Halil Isilar Middle School

Abstract

For the natural number $n > 1$, Euler function gives the amount of natural numbers smaller than and coprime to n. However, there is no study to find out what these numbers are. In this study, the solution method of this problem which the Euler Function cannot respond to has been found. In this method, Groups, Cyclic Groups, Group Homomorphism and Group Isomorphism are used. In addition, Modular Arithmetic and Chinese Remainder Theorem were used. Thanks to the method found, at least two-levels encryption algorithm has been developed. In this algorithm, it is aimed to prevent related companies from backing up, especially in social media and various communication applications such as WhatsApp.

Keywords: Abstract Algebra, Algorithm, Chinese Remainder Theorem, Cyclic Group, Group Isomorphism

1. Introduction

For the natural number $n > 1$,

$n=a^x.b^y.c^z$................................. is number n's prime factorization;

$\phi(n)=(a^x-a^{x-1}).(b^y-b^{y-1}).(c^z-c^{z-1})$.................. value is found by the formula.

- When n is prime number; $\phi(n)= n-1$
- When n is the odd natural number; $\phi(2n)= \phi(n)$
- When n is an even natural number; $\phi(2n)=2.\phi(n)$
- When $n=2^k$, $k\in Z^+$; $\phi(n)= \frac{n}{2}$

Euler function gives the amount of natural numbers smaller than and coprime integer to n. There is no study on the values of these numbers. This problem, which the Euler function cannot answer, is emphasized. In order to find these numbers, firstly; the generators of two isomorphic groups were acted on. Later in the study for three or more isomorphic groups; An encryption algorithm was tried to be developed based on its generators.[1]

2. Method

2.1 Group and Group Types

In the (G, Δ) binary operation, the transaction that satisfies the following conditions specifies a group.

For ∀a, b ∈ G; a Δ b ∈ G expression, that is, the closure property must be provided.

• For ∀a ∈ G, it must be e ∈ G, which provides aΔe = eΔa = a, and this element is called a neutral (unit) element.

• The element a^{-1} ∈ G that provides "$a\Delta a^{-1}=a^{-1}\Delta a=e$" for ∀a ∈ G is the inverse element.

• For ∀a, b, c ∈ G; (aΔb) Δc=aΔ(bΔc) associative property must be provided. Binary operations that provide these features are called abelian groups.[2]

2.1.1 Z_n Total Groups

The (Z,+) Total group is a group under addition process defined in integers.

(Z_n, +) Total group is the group that accepts the remainder class of the number n.

The set $Z_7=\{\bar{0},\bar{1},\bar{2},\bar{3},\bar{4},\bar{5},\bar{6}\}$ is the group formed under the addition process.

2.1.2 Cartesian Product Groups

(Z_n X Z_m, +) group is the additive group that accepts the Cartesian product of $Z_n=\{\overline{0},\overline{1},\overline{2},\ldots\ldots\ldots,\overline{n-1}\}$ and $Z_m=\{\overline{0},\overline{1},\overline{2},\ldots\ldots\ldots,\overline{m-1}\}$ sets. Similarly, the Cartesian Product group can be written eternally as Z_n X Z_m X Z_p , Z_n X Z_m X Z_p X $Z_{t\ldots}$.

2.1.3 Cyclic Groups

In group (G, ∗), it is called the group that satisfies the condition of <$\bar{a}$> including ∃a ∈G. The elements "a" in this group are called generators. If a group is cyclic, it must be an abelian group.

2.2 Group Homomorphism

Let (G, Δ) and (H, ∗) be two groups.

$f: G \to H$, f function, $f: H \to G$

$\forall$a, b $\in$ G; If $f(a \Delta b) = f(a) * f(b)$ satisfies the condition, it is called group homomorphism.

- If the f function is the Overlying Function; It is called epimorphism.
- If the domain and image set are the same, the f function is called atomorphism.
- If f function is injective and onto function; called isomorphism.

2.2.1 Group Isomorphism

For the isomorphism defined as $f: G \to H$, the following can be said;

- The G and H groups either both of the groups are cyclic groups or none are.
- Both groups must be either abelian groups or non-abelian groups.
- The order of the two groups must be the same.
- Both groups must be either countable groups or uncountable groups.

2.3 Properties of two isomorphic and cyclic groups

Let (G, Δ) and (H,$*$) be two cyclic groups. If these two groups are isomorphic, the number of generators of both groups is the same. In addition, the generators in both groups match exactly.

2.4 Z_n and Z_m X Z_p Cyclic-Isomorph Groups

Numbers that are smaller than n and coprime numbers to n, are actually generators of the Z_n group. If we find an isomorph Z_m X Z_p group to the Z_n group, we can analyze the relation between its generators.

Example1: Z_6 and Z_2 X Z_3 groups are isomorphic to each other. Let's create the group table of both groups.

Z_6	$\overline{1}$	$\overline{2}$	$\overline{3}$	$\overline{4}$	$\overline{5}$	$\overline{0}$
$\overline{1}$	$\overline{2}$	$\overline{3}$	$\overline{4}$	$\overline{5}$	$\overline{0}$	$\overline{1}$
$\overline{2}$	$\overline{3}$	$\overline{4}$	$\overline{5}$	$\overline{0}$	$\overline{1}$	$\overline{2}$
$\overline{3}$	$\overline{4}$	$\overline{5}$	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$
$\overline{4}$	$\overline{5}$	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$	$\overline{4}$
$\overline{5}$	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$	$\overline{4}$	$\overline{5}$
$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$	$\overline{4}$	$\overline{5}$	$\overline{0}$

(Table-1)

Z_2XZ_3	$(\overline{1},\overline{1})$	$(\overline{0},\overline{2})$	$(\overline{1},\overline{0})$	$(\overline{0},\overline{1})$	$(\overline{1},\overline{2})$	$(\overline{0},\overline{0})$
$(\overline{1},\overline{1})$	$(\overline{0},\overline{2})$	$(\overline{1},\overline{0})$	$(\overline{0},\overline{1})$	$(\overline{1},\overline{2})$	$(\overline{0},\overline{0})$	$(\overline{1},\overline{1})$
$(\overline{0},\overline{2})$	$(\overline{1},\overline{0})$	$(\overline{0},\overline{1})$	$(\overline{1},\overline{2})$	$(\overline{0},\overline{0})$	$(\overline{1},\overline{1})$	$(\overline{0},\overline{2})$
$(\overline{1},\overline{0})$	$(\overline{0},\overline{1})$	$(\overline{1},\overline{2})$	$(\overline{0},\overline{0})$	$(\overline{1},\overline{1})$	$(\overline{0},\overline{2})$	$(\overline{1},\overline{0})$
$(\overline{0},\overline{1})$	$(\overline{1},\overline{2})$	$(\overline{0},\overline{0})$	$(\overline{1},\overline{1})$	$(\overline{0},\overline{2})$	$(\overline{1},\overline{0})$	$(\overline{0},\overline{1})$
$(\overline{1},\overline{2})$	$(\overline{0},\overline{0})$	$(\overline{1},\overline{1})$	$(\overline{0},\overline{2})$	$(\overline{1},\overline{0})$	$(\overline{0},\overline{1})$	$(\overline{1},\overline{2})$
$(\overline{0},\overline{0})$	$(\overline{1},\overline{1})$	$(\overline{0},\overline{2})$	$(\overline{1},\overline{0})$	$(\overline{0},\overline{1})$	$(\overline{1},\overline{2})$	$(\overline{0},\overline{0})$

(Table-2)

When two group tables are examined,

- In the top row, the generators are in the same place and match one each.
- The positions of the generators in the group tables are the same and match exactly.

2.5 Finding Z_n Generator from Cartesian Product Group generator

Let there be two isomorphic groups. We can find the generator in the Z_n group of a generator taken from the cartesian product group.

Example2: Let's find a number coprime to and smaller than 60.

Solution2: Z_{60} group and Z_4 X Z_{15} group are isomorphic to each other. Let's get a generator from the group Z_4 X Z_{15}. Generator (3,7) is actually the generator that is formed in the group table Z4 X Z15 by summing the number (1,1) n times.

n. $(\bar{1},\bar{1}) \equiv (\bar{3},\bar{7})$ (mod(4,15))

(n,n) $\equiv(\bar{3},\bar{7})$ (mod(4,15)) $\Rightarrow$ n$\equiv 3(mod4)$

n$\equiv 7(mod15)$

n$\equiv \bar{3}(mod4) \Rightarrow n = 4k+3, k \in Z$………………(1)

n$\equiv \bar{7}(mod15) \Rightarrow n = 4k+3 \equiv 7\ (mod15)$

$\Rightarrow 4k \equiv 4\ (mod15)$

$\Rightarrow k \equiv 1\ (mod15)$

$\Rightarrow k = 15m+1, m \in Z$ …………..(2)

If (1) in (2) is written in place;

It is n= $4k+3 = 4(15m+1)+3 = 60m+7$.

Example3: Let's find a number coprime to and smaller than 120.

Solution3: The group isomorphic to the Z_{120} group is Z_3 X Z_5 X Z_8.

Let's take a generator from the cartesian product group. Let this generator $(\overline{2},\overline{3},\overline{7})$.

$n.(\overline{1},\overline{1},\overline{1}) \equiv (\overline{2},\overline{3},\overline{7})$(mod(3,5,8))

n$\equiv 2(mod3)$

n$\equiv 3(mod5)$

It is n$\equiv 7(mod8)$.

n$\equiv 2(mod3) \Rightarrow n = 3k+2, k \in Z$………………(3)

$3k+2 \equiv 3(mod5) \Rightarrow 3k \equiv 1(mod5)$

$\Rightarrow k \equiv 2(mod5)$

$$\Rightarrow k = 5t + 2, t \in Z \ldots\ldots\ldots\ldots(4)$$

If (3) in (4) is written in place;

$n = 3(5t + 2) + 2 = 15t + 8$

$n = 15t + 8 \equiv 7(mod8) \Rightarrow 15t \equiv -1(mod8)$

$$\Rightarrow -t \equiv -1(mod8)$$

$$\Rightarrow t \equiv 1(mod8)$$

$$\Rightarrow t = 8m + 1, m \in Z \ldots\ldots\ldots(5)$$

It is $n = 15(8t + 1) + 8 = 120t + 23$. In Z_{120}; 23 was found as generator. 23 and 120 are coprime numbers.

3. Results

Numbers, which smaller than n>1 natural number and coprime to n; if Z_n group and Z_m X Z_p X Z_t Cartesian product group is isomorphic to each other, it can be found easily with the help of generators. It can also be written as a function.

Example 4: Let Z_n group and Z_m X Z_p X Z_t group be isomorphic groups. Taken from the cartesian product group $(\overline{y}, \overline{z}, \overline{r})$; for all generators,

$$f(x) = \begin{cases} x \equiv y(mod\ m) \\ x \equiv z(mod\ p) \\ x \equiv r(mod\ t) \end{cases}$$

The function $f(x)$ is the function that gives the coprime to and smaller than n.

3.2 Reaching Zn group from cartesian product groups

n = p.q.r.m.t.x.y,

Let Z_p X Z_q X Z_r X Z_m X Z_t X Z_x X Z_y Cartesian product be an isomorph to the Z_n group. For the generator $(\overline{a}, \overline{b}, \overline{c}, \overline{d}, \overline{e}, \overline{f}, \overline{g})$ taken from the cartesian product group,

The generator can find in the group $Z_{p.q}$ X Z_r X Z_m X Z_t X Z_x X Z_y.

The generator can find in the group $Z_{p.q.r}$ X Z_m X Z_t X Z_x X Z_y.

The generator can find in the group $Z_{p.q.r.m}$ X Z_t X Z_x X Z_y.

The generator can find in the group $Z_{p.q.r.m.t}$ X Z_x X Z_y.

The generator can find in the group $Z_{p.q.r.m.t.x}$ X Z_y.

The generator can find in the group $Z_{p.q.r.m.t.x.y} = Z_n$.

This number gives the numbers coprime to and smaller than n.

3.3 Creating an Algorithm

This algorithm is primarily prepared at the simplest level. Different forms of this algorithm are described in detail in Section 4. While creating the character code table to be used in this algorithm, ASCII characters are coprime to and smaller than 816; Character table was made by matching from small to large numbers respectively.

CODE	CHAR	CODE	CHAR	CODE	CHAR	CODE	CHAR	CODE	CHAR	CODE
1	(nul)	139	+	277	W	443	Ê	589	╣	707
5	(soh)	143	,	281	X	445	Ô	593	║	709
7	(stx)	145	-	283	Y	449	Ó	599	╗	713
11	(etx)	149	.	287	Z	451	ı	601	╝	715
13	(eot)	151	/	293	[	455	ƒ	605	╜	719
19	(enq)	155	0	295	\	457	≈	607	╛	721
23	(ack)	157	1	299	]	461	...	611	┐	725
25	(bel)	161	2	301	^	463	Ê	613	└	727
29	(bs)	163	3	305	_	467	∆	617	┴	733
31	(tab)	167	4	307	,	469	Ù	619	┬	737
35	(lf)	169	5	311	a	473	ˆ	623	├	739
37	(vt)	173	6	313	b	475	Ú	625	─	743
41	(np)	175	7	317	c	479	°	631	┼	745
43	(cr)	179	8	319	d	481	ˇ	635	╞	749
47	(so)	181	9	325	e	485	0	637	╟	751
49	(si)	185	:	329	f	487	Ö	641	╚	755
53	(dle)	191	;	331	g	491	Ü	643	╔	757
55	(dc1)	193	<	335	h	497	-	647	╩	761
59	(dc2)	197	=	337	i	499	£	649	╦	763
61	(dc3)	199	>	341	j	503		653	╠	767
65	(dc4)	203	?	343	k	505	Ş	655	═	769
67	(nak)	205	@	347	l	509	Ş	659	╬	773
71	(syn)	209	A	349	m	511	.	661	╧	775
73	(etb)	211	B	353	n	515	İ	665	╨	779
77	(can)	215	C	355	o	517	Û	667	╤	781
79	(em)	217	D	359	p	521	·	671	╥	785
83	(eof)	223	E	361	q	523	Ò	673	╙	787
89	(esc)	227	F	365	r	529	□	677	╘	791
91	(fs)	229	G	367	s	533		679	╒	793
95	(gs)	233	H	371	t	535	ğ	683	╓	797
97	(rs)	235	I	373	u	539	TL	685	╫	803
101	(us)	239	J	377	v	541		689	╪	805
103	sp	241	K	379	w	545	"	691	┘	809
107	!	245	L	383	x	547	Ω	695	┌	811
109	ì	247	M	385	y	551	º	701	█	815
113	#	251	N	389	z	553	0	703	▄	
115	$	253	O	395	{	557	′			
121	%	257	P	397		559	ª			
125	&	259	Q	401	}	563	░			
127	ë	263	R	403	~	565	▒			
131	(	265	S	407		569	▓			
133	)	269	T	409	Ç	571	│			
137	*	271	U	413	ü	575	┤			
		275	V	415	È	577	╡			
				419	‚	581	╢			
				421	‰	583	╖			
				427	‡	587	╕			
				431	Â					
				433	ç					
				437	Í					
				439	Î					

(Table-3)

As can be seen in Table-3, while the number 816 is chosen, it is aimed to have 256 coprime numbers. Because the number of ASCII characters is 256.

3.3.1 First encryption with Z_3 X Z_{16} X Z_{17} group

In this encryption, firstly, character codes in Table-3 created according to the generators of the Z_{816} group that is isomorphic to this group will be used.

Example 5: Let's encrypt the word "Ahmet" in the given group. First of all, the character codes of the letters are as follows; A = 205, h = 365, m = 347, e = 319, t = 371. Since these numbers are generators of the Z_{816} number, the matching generators in Z_3 X Z_{16} X Z_{17} will be passwords.

- When $205.(\overline{1},\overline{1},\overline{1}) \equiv (\overline{x},\overline{y},\overline{z})(mod(3,16,17))$ is found, the generator becomes (1,13,1).
- When $365.(\overline{1},\overline{1},\overline{1}) \equiv (\overline{x},\overline{y},\overline{z})(mod(3,16,17))$ is found, the generator becomes (2.13.8).

When the operations are continued;

CHARACTER	TEXT ENCRYPTION
A	**(1,13,1)**
h	**(2,13,8)**
m	**(2,11,7)**
e	**(1,15,13)**
t	**(2,3,14)**

(Table-4)

It is encrypted in Table-4.

3.3.1.2 decrypting the Z_3 X Z_{16} X Z_{17} group

Each password in Table-4, the generator, has the generator in Z_{816}. The value of this generator makes it possible to find out which character corresponds to from the character code table.

Example-6: Let's find out which character the password in Table-4 (2,13,8) belongs to.

$x \equiv 2(mod3)$

$x \equiv 13(mod16)$

$x \equiv 8(mod17)$.

$x \equiv 2(mod3) \Rightarrow x = 3k + 2, k \in Z$..................(6)

$x \equiv 13(mod16) \Rightarrow 3k + 2 \equiv 13\ (mod16)$

$\Rightarrow 3k \equiv 11\ (mod16)$

$\Rightarrow 3k \equiv 27\ (mod 16)$

$\Rightarrow k \equiv 9\ (mod 16)$

$\Rightarrow k = 16m + 9, m \in Z$…………………………..(7)

If (7) in (6) is written in place;

$x = 3.(16m + 9) + 2$

$x = 48m + 29$…………………………………..(8)

$x = 48m + 29 \equiv 8\ (mod 17)$

$\Rightarrow 14m \equiv -21\ (mod 17)$

$\Rightarrow -3m \equiv -21\ (mod 17)$

$\Rightarrow m \equiv 7\ (mod 17)$

$\Rightarrow m = 17p + 7, p \in Z$……………………….(9)

If (9) in (8) is written in place;

$x = 48.(17p + 7) + 29$

$x = 816p + 365$.

The number 365 becomes the generator in Z816 and is the code of the letter "h" in Table-3.

3.3.2.1 Second (level) encryption in Z_{48} X Z_{17} group

Character codes received according to the Z_{816} group are encrypted according to the Z_3 X Z_{16} X Z_{17} group. The encrypted text is encrypted again according to the Z_{48} X Z_{17} group.

Example-7: Let's find the equivalent of the generator $(\overline{2}, \overline{11}, \overline{7})$, which is the encrypted version of the letter "m" in Table-4, to the generator in Z_{48} X Z_{17}.

$x \equiv 2(mod 3)$

$x \equiv 11(mod 16)$

$x \equiv 2(mod 3) \Rightarrow x = 3k + 2, k \in Z$…………………..(10)

$3k + 2 \equiv 11(mod 16)$

$3k \equiv 9(mod 16)$

$k \equiv 3\ (mod 16) \Rightarrow k = 16t + 3, t \in Z$…………………(11)

If (11) in (10) is written in place;

$x = 3(16t + 3) + 2 = 48t + 11.$

The number 11 is found as a generator in Z_{48}.

Accordingly, the second encryption is made in the case of $(\overline{2}, \overline{11}, \overline{7}) \rightarrow (\overline{11}, \overline{7})$.

CHARACTER	CHARACTER CODE	Encrypted text according to Z_3 X Z_{16} X Z_{17}	Encrypted text according to Z_{48} X Z_{17}
A	205	(1,13,1)	(13,1)
h	365	(2,13,8)	(29,8)
m	347	(2,11,7)	(11,7)
e	319	(1,15,13)	(31,13)
t	371	(2,3,14)	(35,14)

(Table-5)

3.3.2.2 Decryption in Z_{48} X Z_{17} Group

When the text encrypted for the second time in Z_{48} X Z_{17} group is decoded according to Z_{816}, it is decrypted.

Example-8: In Table-5, let's decrypt the encrypted character (31,13).

$x \equiv 31(mod48)$

$x \equiv 13(mod17)$

$x \equiv 31(mod48) \Rightarrow x = 48t + 31, t \in Z$…………………(12)

$48t + 13 \equiv 13(mod17)$

$-3t \equiv -28(mod17)$

$-3t \equiv -11(mod17)$

$t \equiv \frac{11}{3}(mod17)$

$t \equiv 15(mod17) \Rightarrow t = 17m + 15, m \in Z$…………………(13)

If (13) in (12) is written in place;

$x = 48(17m + 15) + 31 = 816m + 319.$

The number 319, which is the generator in the Z_{816} group, is the code of the letter "e" in the character code table.

4. Conclusion and Discussion

The following results were reached in this study;

- First of all, the value of coprime numbers to and smaller than n can be found the number n, which the Euler function cannot respond to. The important thing here is that there is an isomorphic cartesian product to the Z_n group for the number n.

- When an isomorphic, cartesian product group is found to Z_n group, the function giving the coprime numbers can be created from the generators of the Cartesian product group.

For example; Let Z_n be an isomorph to Z_m X Z_p X Z_q group. The function that gives coprime numbers;

$$f(x) = \begin{cases} x \equiv a(mod\ m), & (\overline{a}, m) = 1 \\ x \equiv b(mod\ p), & (b, p) = 1 \\ x \equiv c(mod\ q), & (c, q) = 1 \end{cases}$$

The same function can be created with quart or more Cartesian product groups.

• The reasons for taking Z_{816} group while creating the algorithm can be explained as follows;

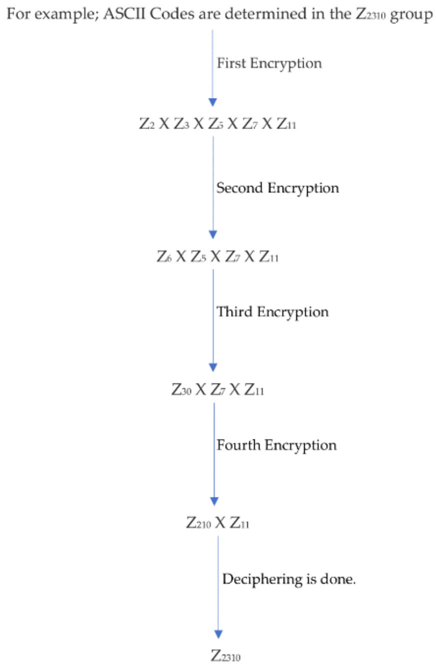
1. ϕ(816)=256, ASCII characters are 256.

2. The Z_{816} group is isomorphic to the Z_3 X Z_{16} X Z_{17} group, and isomorphic to the Z_{48} X Z_{17} group. Two levels encryption can be done.

- For the whole character of a text in the created algorithm, the generators of the Z_3 X Z_{16} X Z_{17} group are written and the first encryption is made, then the encrypted text is encrypted again in Z_{48} X Z_{17} and sent to the third person.

- Thanks to this encryption, the second person, who is called the intermediary, encrypts it differently without deciphering password and sends it to the receiver. Especially when the software is made, the company, which is an intermediary in applications such as WhatsApp, cannot make backups.

• It is not necessary to take the Zn group as Z_{816} in this encryption algorithm. A very large number n is chosen such that the Cartesian product group can contain more than three Cartesian products. Here, 256 numbers of n and coprime numbers can be selected and given to ASCII Characters as codes. In this way, more than two encryptions can be made.



(Template-1)

References

[1]. D. Tasci, Abstract Algebra, 2007.

[2]. F. Callialp, Abstract Algebra with Examples, 2013.

[3]. Charles C. Pinter, A book of Abstract Algebra, 1982.

[4]. Jonathan D. H. Smith, Introduction to Abstract Algebra, 2008.