Algologic Technical Report # 04/2012

Group theoretic view of modulo arithmetic

S. Parthasarathy[1]
drpartha@gmail.com

Ref.: modulogroup1.tex
Ver.: 20120308

Abstract

This report is a tutorial introduction to the role of algebra in cryptography which involves modular arithmetic. This report is based on a companion report [2]. The concept of an algebraic group (aka group), is fairly well known. This concept can be extended to sets involving modular arithmetic. Such algebraic properties find a useful role in cryptography.

Contents

[1]Algologic Research and Solutions, 78 Sancharpuri Colony, Bowenpally, Secunderabad 500 011, India WWW-URL – http://algolog.tripod.com/nupartha.htm

Group theoretic view of modulo arithmetic

1 Basic definitions and conventions

In the text that follows, we use the term *modulo* as an adjective, and the term *modular* as an adverb. Thus we say *modulo arithmetic* (since arithmetic is a noun), and *modular addition* (addition denotes the verb "to add") or *modular multiplication* (multiplication denotes the verb "to multiply").

1. $\mathbb{Z}$ Denotes the set of integers {..., -2, -1, 0, 1,2,3,4,....}
2. $\mathbb{Z}^+$ Denotes the set of positive integers {1,2,3,4,....}
3. $\mathbb{Z}_m$ Denotes the set of residues (remainders) when any $z \in \mathbb{Z}$ is divided by m. $\mathbb{Z}_m = \{0, 1, 2, 3, 4, 5, ...m-1\}$
   For example,
   $\mathbb{Z}_3$ = 0, 1, 2
   $\mathbb{Z}_4$ = 0, 1, 2, 3
   $\mathbb{Z}_5$ = 0, 1, 2, 3, 4 etc.
4. Given $a, m, n \in \mathbb{Z},\ n = a.\ mod\ m$ if n is the remainder when a is divided by m. We can express this by $a = k.m + n$ where $a, k, m, n \in \mathbb{Z}$.
5. Let m be a positive integer. We say that two integers x and y are $congruent\ modulo\ m$, and write $x \equiv y\ mod\ m$, in case m divides x - y. This property is written as $m|(x$ - $y)$. i.e. $m \equiv 0\ mod\ (x-y)$

   Thus $x \equiv y\ mod\ m$ if and only if there is $k \in \mathbb{Z}$ such that x - $y = km$

   $x \equiv y\ mod\ m$ is also written as $x \equiv_m y$
6. We will be using two fundamental relationships in modular arithmetic ::

   Let $a \equiv b(mod\ m)$ and $c \equiv d(mod\ m)$

$$a + c = (b+d)\ mod\ m \tag{1}$$
$$ac = bd\ mod\ m \tag{2}$$

   Proof :

$$a \equiv b(mod\ m) \implies b = a + sm \quad s \in \mathbb{Z}^+ \tag{3}$$
$$c \equiv d(mod\ m) \implies d = c + km \quad k \in \mathbb{Z}^+ \tag{4}$$

Adding equation 3 and 4 we get

$$b \ + \ d \ = \ (a+c) \ + \ m(s+k) \tag{5}$$
$$\tag{6}$$

which implies

$$a+c \ = \ (b+d) \ mod \ m \tag{7}$$

QED

Multiplying equation 3 and 4 we get

$$b.d \ = \ (a+sm).(c+km) \tag{8}$$
$$= a.c + akm + csm + sm.tm \tag{9}$$
$$= a.c + m.(ak + cs + stm) \tag{10}$$

which implies

$$a.c = b.d \ mod \ m \tag{11}$$

QED

2 Groups

In mathematics, and more specifically abstract algebra, the term algebraic structure generally refers to an arbitrary set with one or more binary operations defined on it. This idea effectively brings out the algebraic properties of the members of the set, and in turn defines an overall structure. Common examples of structures include groups, rings, fields and lattices. More complex algebraic structures can be defined by introducing multiple operations, different underlying sets, or by altering the defining axioms. Examples of more complex structures include vector spaces, modules and algebras.

A group is a set, G, together with an operation $\star$ (called the group law of G) that combines any two elements a and b to form another element, denoted $a \star b$ or ab. To qualify as a group, the set and operation, $< G, \star >$, must satisfy four requirements known as the group axioms:

1. CLOSURE: If a and b are in the group then $a \star b$ is also in the group.

2. ASSOCIATIVITY: If a, b and c are in the group then $(a \star b) \star c = a \star (b \star c)$.

3. IDENTITY: There is an element e of the group such that for any element a of the group $a \star e = e \star a = a$.

4. INVERSES: For any element a of the group there is an element a^{-1} such that
$a \star a^{-1} = e$
and
$a^{-1} \star a = e$

2.1 Abelian Groups

Abelian Groups, named after Niels Henrik Abel (5 August 1802 6 April 1829), are a special class of groups.

In abstract algebra, an abelian group, also called a commutative group, is a group in which the result of applying the group operation to two group elements does not depend on their order (the axiom of commutativity). Abelian groups generalize the arithmetic of addition of integers.

In the case of abelian groups, we extend the above axioms by adding one more property to the above axioms :

COMMUTATIVITY : For all a, b in A, $a \star b = b \star a$.

One of the most familiar groups is $< \mathbb{Z}, + >$ Where $\mathbb{Z}$ is the set of integers :

..., 4, 3, 2, 1, 0, 1, 2, 3, 4, ..

and $+$ is the integer addition operation.

The following properties of integer addition serve as a model for the abstract group axioms given in the definition below.

1. For any two integers a and b, the sum a + b is also an integer. Thus, adding two integers never yields some other type of number, such as a fraction. This property is known as closure under addition.

2. For all integers a, b and c, (a + b) + c = a + (b + c). Expressed in words, adding a to b first, and then adding the result to c gives the same final result as adding a to the sum of b and c, a property known as associativity.

3. If a is any integer, then 0 + a = a + 0 = a. Zero is called the identity element of addition because adding it to any integer returns the same integer.

4. For every integer a, there is an integer b such that a + b = b + a = 0. The integer b is called the inverse element of the integer a and is denoted a.

5. For every integer a and b, a + b = b + a

Note : For a given set $\mathbb{Z}$, there may be many binary operations on members of $\mathbb{Z}$ e.g. given $\mathbb{Z}$, the set of integers, we can have binary operations + - or * / Can all of these operations be used for creating a group ?

$<\mathbb{Z}$, $+>$ satisfies all 4 group axioms. So, $<\mathbb{Z}$, $+>$ forms a group. $<\mathbb{Z}$, $+>$ is an Abelian group, since a+b=b+a for all a,b belonging to $\mathbb{Z}$

$<\mathbb{Z}$, -> does not satisfy all 4 group axioms. For instance. $a-(b-c) \neq (a-b)-c$ (associativity axiom). So, $<\mathbb{Z}$, -> does not form a group

$<\mathbb{Z}$, *> Does not satisfy Axiom 4 (existance of inverse). All integers belonging to $\mathbb{Z}$, except 1, do not have an integer multiplicative inverse (in $\mathbb{Z}$)

$<\mathbb{Z}$, / > does not satisfy the group axioms for closure property

Now let us study the set $\mathbb{Z}^+$ and the four operations +,-,*,/

$<\mathbb{Z}^+$, $+>$ forms a group.

$<\mathbb{Z}^+$, -> Does not form a group . Why ? (try 4-7).

$<\mathbb{Z}^+$, *> Forms a group.

$<\mathbb{Z}^+$, / > Does not form a group . Why ? (try 4 / 7)

Exercise for the reader (you !): Which of the above are Abelian groups ?

3 Modulo arithmetic

Extending the above ideas to sets of integers which are subject to reductio modulo m, gives interesting results.

We notice that $\mathbb{Z}_n$ is a subset of $\mathbb{Z}$. Thus, any integer $x \in \mathbb{Z}$ can be mapped to $\mathbb{Z}_n$ by dividing by n and taking the residue, this is called reduction modulo n, and the resulting residue is called x mod n. So any $x \in \mathbb{Z}$ corresponds to an element in $\mathbb{Z}_n$ via reduction mod n. For instance, if n = 3, then the numbers ...3, 0, 3, 6, .. all correspond to 0 in $\mathbb{Z}_3$, while ..., 2, 1, 4, ... all correspond to 1, etc. For any n, we can split the integers into classes, according to which element in $\mathbb{Z}_n$ they correspond to. There will be exactly n classes. Numbers in the same class are said to be congruent modulo n. So 1 and 4 are congruent mod 3, this is written as $1 \equiv 4 mod 3$, while 0 and 5 are not.

We can now define addition and and multiplication of numbers in $\mathbb{Z}_n$ in a special way, so we get results that are also in $\mathbb{Z}_n$. From numbers a, b $\in \mathbb{Z}$, we can compute a new number called $(a+b)modn$ (also written as a+b mod n), which is also in $\mathbb{Z}_n$, as follows: compute a + b, divide by n and let a + b mod n be the residue. Since we divide by n, the residue will always be in Zn .

Multiplication can be done in a similar way, ab mod n is by definition the residue we get when dividing ab by n.

For instance, 3 + 4 mod 5 = 2, 3 * 3 mod 5 = 4.

Let us create two matrices in $\mathbb{Z}_5$. Matrix A_5 (addition matrix) denotes addition in modulo 5 arithmetic, matrix M_5 (multiplication matrix) denotes multiplication in modulo 5 arithmetic

+	0	1	2	3	4
0	0	1	2	3	4
1	1	2	3	4	0
2	2	3	4	0	1
3	3	4	0	1	2
4	4	0	1	2	3

Table 1: $\mathbb{A}_5$ Modular addition in $\mathbb{Z}_5$

*	0	1	2	3	4
0	0	0	0	0	0
1	0	1	2	3	4
2	0	2	4	1	3
3	0	3	1	4	2
4	0	4	3	2	1

Table 2: $\mathbb{M}_5$ Modular multiplication in $\mathbb{Z}_5$

In other words,
$A_5(i,j) = (a(i,1) + a(1,j))mod\ 5$
$M_5(i,j) = (m(i,1) * m(1,j))mod\ 5$

Now, let us create two matrices in $\mathbb{Z}_6$. Matrix A_6 (addition matrix) denotes

addition in modulo 6 arithmetic, matrix M_6 (multiplication matrix) denotes multiplication in modulo 6 arithmetic

+	0	1	2	3	4	5
0	0	1	2	3	4	5
1	1	2	3	4	5	0
2	2	3	4	5	0	1
3	3	4	5	0	1	2
4	4	5	0	1	2	3
5	5	0	1	2	3	4

Table 3: $\mathbb{A}_6$ Modular addition in $\mathbb{Z}_6$

*	0	1	2	3	4	5
0	0	0	0	0	0	0
1	0	1	2	3	4	5
2	0	2	4	0	2	4
3	0	3	0	3	0	3
4	0	4	2	0	4	2
5	0	5	4	3	2	1

Table 4: $\mathbb{M}_6$ Modular multiplication in $\mathbb{Z}_6$

In other words,
$A_6(i,j) = (a(i,1) + a(1,j))mod\ 6$
$M_6(i,j) = (m(i,1) * m(1,j))mod\ 6$

3.1 Modular addition

Observe the matrices A_5 and A_6. A "0" in the position a(i,j) would mean that a(i,1) + a(1,j) = 0. This is the modular arithmetic equivalent of additive inverse in traditional integer arithmetic. Notice that two positive integers can never add up to 0 in traditional integer arithmetic. Whereas this is possible in modular arithmetic. 5+1= 6 in traditional integer arithmetic, 5+1 = 6 mod 6 = 0 in mod 6 arithmetic.

Notice that every row of A_5 and every row of A_6 has at least one "0". Notice that every column of A_5 and every column of A_6 has at least one "0". This observation implies every element of Z_5 and every element of Z_6 has an additive inverse respectively in Z_5 or Z_6 . "0" also belongs to Z_5 and Z_6. Modular addition of any element $x \in A$ to any element $y \in A$ results in an element c which is also in A. This is the *closure* property of modular additive inverse.

3.2 Modular multiplication

Observe the matrices M_5 and M_6. A "1" in the position a(i,j) would mean that m(i,1) * m(1,j) = 1. This is the modular arithmetic equivalent of multiplicative inverse in traditional integer arithmetic. Notice that the product of two non zero

integers can never result in a "1" in traditional integer arithmetic. Whereas this is possible in modular arithmetic. 2*3 = 6 in traditional integer arithmetic, 2*3 = 6 mod 5 = 1 in mod 5 arithmetic. 2 is the multiplicative modular inverse of 3 (and vice versa) in mod 5 arithmetic.

In modulo 6 arithmetic, we notice that except for 5 and 1, the product of no two elements of A_6 is a "1" This results from the observation that there is no "1" in any of the columns or any of the rows of M_6 (except 5 and 1).

Elements of $\mathbb{Z}_m$ can be grouped into two disjoint sets ::

1. *Units* – Elements with multiplicative inverse. In the case of $\mathbb{Z}_6$, this set would be $\{1,5\}$
2. *Divisors of zero* – Elements which when multiplied by some other non-zero element give "0" as a product. e.g 2*3 =0 mod 6

We can observe that :
gcd (6,1) = 1
gcd (6,5) = 1

The set of integers in $\mathbb{Z}_m$ which are coprime to m is denoted by $\mathbb{Z}_m^*$. Thus, $\mathbb{Z}_6^*$ is $\{1,5\}$.

gcd (6,x) $> 1 \; \forall \; x \in \{0,2,3,4\}$

$\{0,2,3,4\}$ is $\{ \mathbb{Z} \setminus \mathbb{Z}_6^* \}$

4 Group properties of modulo arithmetic

Modulo arithmetic over the set $\mathbb{Z}_m$ offers interesting properties which can be studied using group theory and higher algebra.

4.1 Group properties of modular addition

Assume the set $\mathbb{Z}_m$

Assume x,y $\in \mathbb{Z}_m$

Assume the binary operation of modular addition, denoted by a $\oplus$, over the elements of $\mathbb{Z}_m$ (we do not use the $+$ sign, to distinguish this from traditional

addition of integers)

Question : Does $< \mathbb{Z}_m, \oplus >$ form a group ?

1. CLOSURE: $\forall$ a,b $\in \mathbb{Z}_m$ then $(a \oplus b) \in \mathbb{Z}_m$. This property is trivial to prove.
2. ASSOCIATIVITY: If $a,\ b\ and\ c \in \mathbb{Z}_m$ then $(a \oplus b) \oplus c = a \oplus (b \oplus c)$.
3. IDENTITY: There is an element e of the group such that for any element a of the group $a \oplus e = e \oplus a = a$. In our case, e is "0".
4. INVERSES: For any element a of the group there is an element a^{-1} such that
   $a \oplus a^{-1} = e$
   and
   $a^{-1} \oplus a = e$

   We noticed this property in $\mathbb{A}_5$ and in $\mathbb{A}_6$, shown above. Every row of $\mathbb{A}_5$ and $\mathbb{A}_6$ contains a "0"

Conclusion : We conclude that $< \mathbb{Z}_m, \oplus >$ forms a group. Further, since $(a \oplus b) = (b \oplus a)$ we can conclude that $< \mathbb{Z}_m, \oplus >$ forms a commutative group (Abelian group)

4.2 Group properties of modular multiplication

Assume the set $\mathbb{Z}_m$

Assume x,y $\in \mathbb{Z}_m$

Assume the binary operation of modular multiplication, denoted by a $\star$, over the elements of $\mathbb{Z}_m$ (we do not use the . sign, to distinguish this from traditional multiplication of integers)

Question : Does $< \mathbb{Z}_m, \star >$ form a group ? There are two options for this question :

- Does $< \mathbb{Z}_5, \star >$ form a group ?
- Does $< \mathbb{Z}_6, \star >$ form a group ?

Case #1 $< \mathbb{Z}_5, \star >$

1. CLOSURE: If $\forall$ a,b $\in \mathbb{Z}_5$ then $(a \star b) \in \mathbb{Z}_5$. This property is trivial to prove.

2. ASSOCIATIVITY: If $a,\ b\ and\ c \in \mathbb{Z}_m$ then $(a \star b) \star c = a \star (b \star c)$.

3. IDENTITY: There is an element e of the group such that for any element a of the group $a \star e = e \star a = a$. In our case, e is "1 mod m".

4. INVERSES: For any element a of the group is there an element a^{-1} such that
   $a \star a^{-1} = e$
   and
   $a^{-1} \star a = e$

   Case #2 $< \mathbb{Z}_6, \star >$

   In the case of $< \mathbb{Z}_6, \star >$ Closure, associativity and idenity properties are satisfied. The "inverse" property is not satisfied in $< \mathbb{Z}_6, \star >$ We have shown that not ALL elements of $\mathbb{Z}_6$ have a multiplicative modulo inverse.

   We noticed this property in $\mathbb{M}_6$, shown above. Not every row (or every column) of $\mathbb{M}_6$ contains a "1"

Conclusion :

- We conclude that $< \mathbb{Z}_5, \star >$ forms a group. And, since $(a \star b) = (b \star a)$ we conclude that $< \mathbb{Z}_5, \star >$ forms an Abelian Group.
- We conclude that $< \mathbb{Z}_6, \star >$ does NOT form a group.

5 Role in cryptography

Modular arithmetic finds an important and often used role in cryptography [1].

1. Modular arithmetic allows groups.

2. Cryptography requires hard problems. Some problems become hard with modular arithmetic. For example, logarithms are easy to compute over all integers (and reals), but can become hard to compute when you introduce a modular reduction. Similarly with finding roots.

3. Cryptography is implemented digitally. It is nice if values can't be of arbitrary size. If you work with modular arithmetic, you have guarantees about the largest value you will see and can allocate the correct amount of space to hold values.

6 Concluding Remarks

This report was typeset in LaTeX by the author (using Kile, on a Suse Linux system). The LaTeX source can be obtained from the author, by sending a request to drpartha@gmail.com.

Writing a mathematically rich document, and typesetting it using LaTeX , is a perilous activity. The author welcomes comments, suggestions and remarks (on this report. Please report any flaws, inconsistencies, and ambiguities you may find, to drpartha@gmail.com. The author thanks you in advance, for this gesture. Every such communication will also be personally acknowledged by the author, and taken into account in the next version of this report.

The author will be happy to answer any questions you may have on this subject.

The author thanks all his colleagues, who diplomatically offered no comments on this report. They were polite and abstained from offending me. But, they did cause a huge damage by not stopping me from making a fool of myself in front of the whole world.

See my lament, posted at http://drpartha.wordpress.com/2012/03/08/112012-the-curse-of-academics/ .

References

[1] Véronique Cortier (cortier@loria.fr) , Stéphanie Delaune, and Pascal Lafourcade, *A Survey of Algebraic Properties Used in Cryptographic Protocols*

[2] `S. Parthasarathy`, *Multiplicative inverse in mod(m)*, Algologic Technical Report #1/2012, Feb. 2012.

* * *$_{\text{modulogroup.tex}}$