Cryptographic Finite Fields

Jibi Abraham

COEP TECHNOLOGICAL UNIVERSITY

Shivajinagar, Pune-411 005

(A Unitary Technological University of Govt. of Maharashtra)

Groups, Rings, Fields

- Are the fundamental elements of abstract algebra
- Without understanding the notion of a finite field, you will not be able to understand AES
- Substitution step in AES is based on the concept of a multiplicative inverse in a finite field.
- Without understanding finite fields, you will NOT be able to understand the derivation of the RSA/ECC algorithm for public-key cryptography

Familiar Number Systems

- Groups, Rings and Fields are concerned with sets on whose elements we can operate algebraically
- Perform an operation of two elements of the set and to obtain a third element of the same set itself
- Example Number Systems

$\mathbb{N} = \{0, 1, 2, \dots\}$	the natural numbers
$\mathbb{Z} = \{ m - n \mid m, n \in \mathbb{N} \}$	the integers
$\mathbb{Q} = \{ m/n \mid m, n \in \mathbb{Z},\ n \neq 0 \}$	the rational numbers
$\mathbb{R}$	the real numbers
$\mathbb{C}$	the complex numbers

Group

- Denoted by {G, .} is a set of elements with binary operation "." which obeys the following operations for a pair (a, b):
  - A1: closure: a.b also in G
  - A2: associative law:(a.b).c = a.(b.c)
  - A3: has identity e: e.a = a.e = a
  - A4: has inverses a^{-1}:$a.a^{-1} = e$
- Finite Group: If having a finite number of elements, otherwise, infinite Group

Group: Example - 1

- Is the set of integers Z= {…-3, -2, -1, 0, 1, 2, 3, …} under the addition operation an infinite group?
  - A1: closure: a+b also in G
  - A2: associative law:(a+b)+c = a+(b+c)
  - A3: has identity 0:0+a = a+0 = a
  - A4: has inverses a^{-1}:$a+a^{-1} = a + (-a) = 0$
- Z is an infinite group under addition

Group: Example -2

- Is the set of integers Z= {…-3, -2, -1, 0, 1, 2, 3, …} under multiplication operation a group?
  - A1: closure: a.b also in G
  - A2: associative law:(a.b).c = a.(b.c)
  - A3: has identity 1:1.a = a.1 = a
  - A4: has inverses a^{-1}: $a.a^{-1} = 1$ (only for 1 and -1)
    - There is no integer b such that $bb^{-1} = 1$
- Z is not an infinite group under multiplication

Group: Example-3

- Is "Multiplicative group of nonzero remainders mod 7" a group? $\{1, 2, 3, 4, 5, 6\}$
- Has multiplication as binary group operation
- Has an identity element (product of x and 1 is x)
- Closed under multiplication, e.g.
  $4 \circ 3 = (4 \text{ x } 3) \bmod 7 = 5$
- Closed under inverse, e.g.
  $5^{-1} = 3 \bmod 7$

"Multiplicative group of nonzero remainders mod 7" is a group

×	1	2	3	4	5	6	
1	**1**	2	3	4	5	6	1
2	2	4	6	**1**	3	5	4
3	3	6	2	5	**1**	4	5
4	4	**1**	5	2	6	3	2
5	5	3	**1**	6	4	2	3
6	6	5	4	3	2	**1**	6

Abelian Group

- Forms an **Abelian group** if obey additionally
  - A5: commutative property: a.b = b.a
- Is set of Integers (+ve, -ve and 0) using addition form an infinite Abelian group? Yes
  - A1: closure: a+b also in G
  - A2: associative law:(a+b)+c = a+(b+c)
  - A3: has identity 0:0+a = a+0 = a
  - A4: has inverses a^{-1}:$a+a^{-1} = 0$. The inverse of *a* is -*a*, for all *a* in ***Z***.
  - A5: commutative property: a+b = b+a

Abelian Groups: Example -2

- The set of non-zero real numbers, ***R****, under multiplication Yes
  - A1: closure: axb also in G
  - A2: associative law:(axb)xc = ax(bxc)
  - A3: The identity element of R* under multiplication is 1
  - A4: The inverse of a is 1/a for all a in R*
  - A5: commutative property: axb = bxa

Abelian Group: Example -3

- Suppose S_n is to be the set of permutations of n distinct symbols: {1,2,...,n}. Suppose $\pi, \rho \in S_n$; **permutation operation ρ and a group in S_n is π;**

. Is S_n a group?

- Let G={ 1, 2, 3 } elements then permutation are **3!=6.** These are

$$\begin{pmatrix}1&2&3\\1&2&3\end{pmatrix},\begin{pmatrix}1&2&3\\2&1&3\end{pmatrix},\begin{pmatrix}1&2&3\\3&2&1\end{pmatrix},\begin{pmatrix}1&2&3\\1&3&2\end{pmatrix},\begin{pmatrix}1&2&3\\3&1&2\end{pmatrix},\begin{pmatrix}1&2&3\\2&3&1\end{pmatrix}$$

Abelian Group: Example -3

- Let $\pi_1 = \{3,2,1\}$, $\pi_2 = \{3,1,2\}$, $\rho = \{1,3,2\}$
  - **A1** closure: $\pi_1 \cdot \rho$: $\{3,2,1\} \cdot \{1,3,2\} = \{3,1,2\} \in Sn$
  - **A2** associative law :

$$\pi_2 \cdot (\pi_1 \cdot \rho) = \{3,1,2\} \cdot \{3,1,2\} = \{2,3,1\}$$

$$(\pi_2 \cdot \pi_1) \cdot \rho = (\{3,1,2\} \cdot \{3,2,1\}) \cdot \{1,3,2\}$$

$$= \{2,1,3\} . \{1,3,2\} = \{2,3,1\}$$

Abelian Group: Example -3 (Contd)

- Let $\pi_1 = \{3,2,1\}$, $\pi_2 = \{3,1,2\}$, $\rho = \{1,3,2\}$
  - **A3** identity {1, 2, 3, .., n}∈Sn E.g. ID={1,2,3}
    - {1,2,3} . {1,3,2} ={1,3,2}
    - {1,3,2} . {1,2,3}={1,3,2}
  - **A4** inverse: {1,2,3}·{2,3,1}={2,3,1}
    - $\pi_1 \cdot \pi_1^{-1}$ ={ ={3,2,1}·{3,2,1} = {1,2,3} (ID)
  - **A5** commutative: {3,2,1}·{2,3,1}≠{2,3,1}·{3,2,1}
- So S_n is a group, but not Abelian

Cyclic Group

- Cyclic Group is generated by a single element called a generator of the group
- G is cyclic if every element b $\in$ G is a power of some fixed element a
  - ie $b = a^k$
- Each element can be written as an integer power of *g* in multiplicative notation, or as an integer multiple of *g* in additive notation.
- Example with the operator ".": $a^3 = a.a.a$
- The additive group of integers is an infinite cyclic group generated by the element 1.
- In this case, powers are interpreted additively, so that n is the n^{th} power of 1

Example: Cyclic Group

- Is “Multiplicative group of nonzero remainders modulo 7” a cyclic group?
- $\{1, 2, 3, 4, 5, 6\}$
- Is a cyclic group for the generators 3 and 5.
- Others are not. Example?
- Eg: 2 and powers
- $2^1 \bmod 7 = 2$
- $2^2 \bmod 7 = 4$
- $2^3 \bmod 7 = 1$
- $2^4 \bmod 7 = 2$
- $2^5 \bmod 7 = 4$

$2^6 \bmod 7 = 1$
$2^7 \bmod 7 = 2$
$2^8 \bmod 7 = 4$
$2^9 \bmod 7 = 1$
$2^{10} \bmod 7 = 2$

$3^1 \bmod 7 = 3$
$3^2 \bmod 7 = 2$
$3^3 \bmod 7 = 6$
$3^4 \bmod 7 = 4$
$3^5 \bmod 7 = 5$
$3^6 \bmod 7 = 1$
$3^7 \bmod 7 = 3$
$3^8 \bmod 7 = 2$

Ring

- A ring is denoted by (R, +, x) is a set of elements with two operations (addition and multiplication) which are:
- (A1-A5) obeyed: an abelian group for operation: addition
- Multiplication:
  - M1: has closure: a and b in R then ab is in R
  - M2: is associative: a(bc) = (ab)c
  - M3: distributive over addition: a(b+c) = ab + ac
- A ring is a set in which we can do addition, (hence also subtraction, [a – b = a + (–b)), and multiplication without leaving the set.

Ring: Example - 1

- Is "Z = {..-3, -2, -1, 0, 1, 2, 3, ..} the integers" a ring?
  - A1: closure: a+b also in G
  - A2: associative law:(a+b)+c = a+(b+c)
  - A3: has identity 0:0+a = a+0 = a
  - A4: has inverses a^{-1}:$a+a^{-1} = 0$
  - A5: commutative property: a+b = b+a
  - M1: has closure: a and b in R then ab is in Z
  - M2: is associative: a(bc) = (ab)c
  - M3: distributive over addition: a(b+c) = ab + ac
- Other Rings
  - Q = { m/n | m, n ∈ Z, n 6 = 0 } the rational numbers
  - R: the real numbers
  - C: the complex numbers are rings

Ring: Example -2

- Is N= {0, 1, 2, . . . } the natural numbers a ring for the usual operations: addition and multiplication?
- A3: existence of additive inverses, fails
- For Example: there is no $n \in N$ for which $1 + n = 0$
- N is NOT a ring for addition and multiplication

Commutative Ring and Integral Domain

- A ring forms a **commutative ring,** if obeys
  - M4: commutative multiplication operation
    - ab = ba for all a, b in R
- If M5 and M6 obey, it forms an **integral domain**
  - M5: multiplication operation has an identity element
    - a1 = 1a = a
  - M6: no zero divisors (ab=0 means either a=0 or b=0)
- Set of Integers with usual + and x is an integral domain

Integral Domain: Example -1

- Is set of square matrices of a given dimension an integral domain?
- An integral domain is a commutative ring in which, for any nonzero x, xy=0 only if y=0.
- (ab=0 means either a=0 or b=0). Can we find two nonzero matrices whose product is zero ?
- For N=2, consider: $A = \begin{bmatrix} 1 & 1 \\ 1 & 1 \end{bmatrix}$

$$B = \begin{bmatrix} 1 & -1 \\ -1 & 1 \end{bmatrix}$$

$$AB = \begin{bmatrix} 1-1 & -1+1 \\ 1-1 & -1+1 \end{bmatrix} = \mathbf{0}$$

- Set of square matrices of a given dimension is not an integral domain

Integral Domain: Example -2

- Is the set of even integers, denoted 2Z, with the usual addition and multiplication, an integral domain?
- is a commutative ring
- Not having a multiplicative identity
  - Assume that there were an element $e \in 2Z$ such that $n \cdot e = n$ for all $n \in 2Z$.
  - If $n = 2$, $2e = 2$, from which we deduce that e would have to be 1. Since 1 not belonging to 2Z we have a contradiction
- Not an an integral domain

Field

- A set of numbers denoted by {F, +, x} with two operations which obey:
  - A1: closure: a+b also in G
  - A2: associative law:(a+b)+c = a+(b+c)
  - A3: has identity 0:0+a = a+0 = a
  - A4: has inverses a^{-1}:$a+a^{-1} = 0$
  - A5: commutative property: a+b = b+a
  - M1: has closure: a and b in R then ab is in Z
  - M2: is associative: a(bc) = (ab)c
  - M3: distributive over addition: a(b+c) = ab + ac
  - M4: commutative multiplication ab = ba for all a, b in R
  - M5: multiplication with identity: a1 = 1a = a
  - M6: no zero divisors (ab=0 means either a=0 or b=0)
  - M7: Multiplicative Inverse: a in F, except 0, there exists a^{-1} such that $aa^{-1} = 1$

Field: Example -1

- Set of integers Z= {…-3, -2, -1, 0, 1, 2, 3, …} is not a field because only 1 and -1 have a multiplicative inverse. For no other n, $nn^{-1}=1=n^{-1}n$.
  - Example

$$\frac{3}{2} \notin \mathbb{Z}$$

Field: Example-2

- Is “a rational number n/m where n and m integers and m ≠ 0” a field?
  - A1: closure: a+b also in G
  - A2: associative law:(a+b)+c = a+(b+c)
  - A3: has identity 0:0+a = a+0 = a
  - A4: has inverses a^{-1}:$a+a^{-1} = 0$
  - A5: commutative property: a+b = b+a
  - M1: has closure: a and b in R then ab is in Z
  - M2: is associative: a(bc) = (ab)c
  - M3: distributive over addition: a(b+c)=ab+ac
  - M4: commutative multiplication ab = ba for all a, b in R
  - M5: multiplication with identity: a1 = 1a = a
  - M6: no zero divisors (ab=0 means either a=0 or b=0)
  - M7: Multiplicative Inverse: a in F, except 0, there exists a^{-1} such that $aa^{-1} = 1$

$$\left(\frac{a_1}{b_1}+\frac{a_2}{b_2}\right)+\frac{a_3}{b_3}=\frac{a_1}{b_1}+\left(\frac{a_2}{b_2}+\frac{a_3}{b_3}\right)$$

$$\frac{a}{b}+0=\frac{a}{b}+\frac{0}{1}=\frac{a\times1+0\times b}{b\times1}=\frac{a}{b}$$

$\frac{a}{b}$ has additive inverse $\frac{-a}{b}$

$$\frac{a}{b}+\frac{c}{d}=\frac{ad+bc}{bd}$$

$$\frac{a}{b}\left(\frac{x_1}{y_1}+\frac{x_2}{y_2}\right)=\frac{a}{b}\frac{x_1y_2+x_2y_1}{y_1y_2}=\frac{a\,(x_1y_2+x_2y_1)}{by_1y_2}$$

$$\frac{a}{b}\frac{x_1}{y_1}+\frac{a}{b}\frac{x_2}{y_2}=\frac{ax_1}{by_1}+\frac{ax_2}{by_2}=\frac{ax_1by_2+by_1ax_2}{b^2y_1y_2}=\frac{ax_1y_2+ay_1x_2}{by_1y_2}$$

$$\frac{a}{b}\frac{c}{d}=\frac{ac}{bd}=\frac{ca}{db}=\frac{c}{d}\frac{a}{b}$$

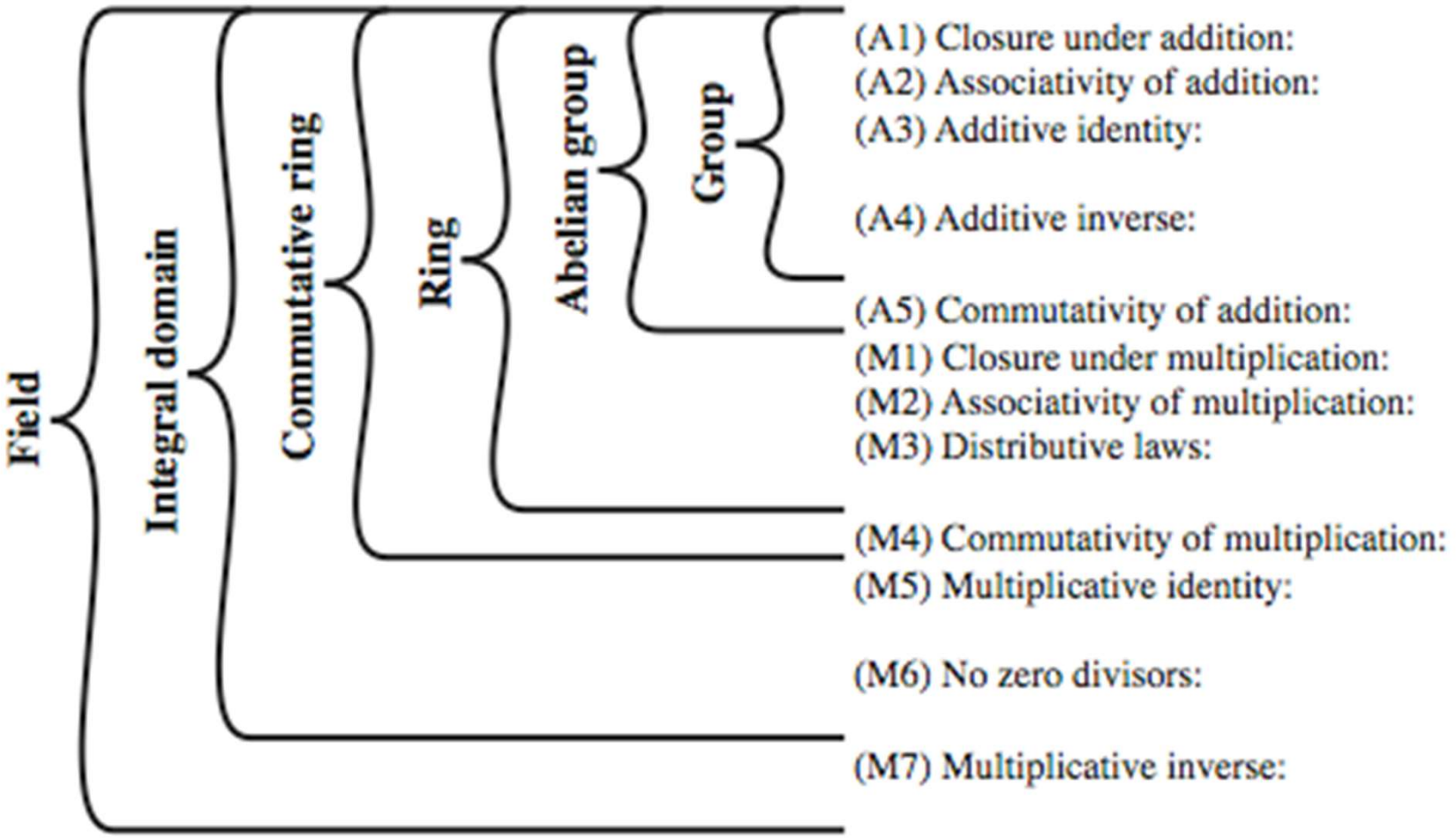
$$\frac{a}{b}\times1=\frac{a}{b}\times\frac{1}{1}=\frac{a\times1}{b\times1}=\frac{a}{b}$$

if $\frac{a}{b}$ is not 0 (equivalently, $a\neq0$), then $\frac{a}{b}$ has inverse $\frac{b}{a}$, which does indeed exist since $a\neq0$

Field:– Example - 3

- E.g. infinite fields: real numbers and complex numbers
- The set of all even integers, positive, negative, and zero, under the operations addition and multiplication
  – is NOT a field.

Groups, Rings, Fields



- Have a hierarchy with more axioms/laws
  - group → ring → fields

Finite Fields used for Cryptography

- Infinite fields are not of interest in cryptography
- Z_n is only a commutative ring and not a finite field is because not every element in Z_n has a multiplicative inverse
- All arithmetic operations must work without error for cryptography
- A finite field is a finite set of numbers in which you can carry out the operations of addition, subtraction, multiplication, and division without error.
- In ordinary computing, division is error-prone and what you see is a high-precision approximation to the true result.
- Such high-precision approximations do not suffice for cryptography work
- Focus in cryptography is on *Prime* fields

Prime Numbers

- Prime numbers only have divisors of 1 and self
  - They cannot be written as a product of other numbers
  - note: 1 is prime, but is generally not of interest
- eg. 2,3,5,7 are prime, 4,6,8,9,10 are not
- Prime numbers are central to number theory
- List of prime number less than 200 is:

```
2 3 5 7 11 13 17 19 23 29 31 37 41 43 47 53 59 61 67
71 73 79 83 89 97 101 103 107 109 113 127 131 137 139
149 151 157 163 167 173 179 181 191 193 197 199
```

Relatively Prime Integers

- **Definition:**
- Two integers a and b are **relatively prime** if gcd(a, b) = 1.

- **Examples:**
- Are 15 and 28 relatively prime?
- Yes, gcd(15, 28) = 1.
- Are 55 and 28 relatively prime?
- Yes, gcd(55, 28) = 1.
- Are 35 and 28 relatively prime?
- No, gcd(35, 28) = 7.

Prime Factorization

- To **factor** a number **n** is to write it as a product of other numbers: **n=a x b x c**
- Factoring a number is relatively hard compared to multiplying the factors together to generate the number
- Is a Fundamental theorem of arithmetic
- **Prime factorization** of a number n is when it is written as a product of primes
  - eg. **91=7x13 ; 3600=2^4x3^2x5^2**
  - 48 = 2x2x2x2x3 = 2^4x3

Divisors

- Say a non-zero number `b` **divides** `a` if for some `m` have `a=mb` (`a,b,m` all integers)
  - $0 \equiv a \bmod b$
- That is `b` divides into `a` with no remainder
- denote this `b|a`
- And say that `b` is a **divisor** of `a`
- eg. all of 1,2,3,4,6,8,12,24 divide 24
- eg. 13 | 182; –5 | 30; 17 | 289; –3 | 33; 17 | 0

Modular Arithmetic

- Define **modulo operator** `a mod n` to be remainder when a is divided by n
  - e.g. 1 = 7 mod 3 ; 4 = 9 mod 5
- Use the term **congruence** for: `a ≡ b (mod n)`
  - when divided by *n,* a & b have same remainder
  - eg. 100 ≡ 34 (mod 11)
- b is called the **residue** of a mod n
  - since with integers can always write: `a = qn + b`
- usually have `0 <= b <= n-1`
  - `-12 mod 7 = -5 mod 7 = 2 mod 7 = 9 mod 7`
  - **n − m** is exactly the same thing as the number **−m mod n**

Modulo 7 Example

```
...
-21  -20  -19  -18  -17  -16  -15
-14  -13  -12  -11  -10   -9   -8
 -7   -6   -5   -4   -3   -2   -1
  0    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
...
```

- all numbers in a column are equivalent (have same remainder) and are called a **residue class**

Modular Arithmetic Operations

- Z_n as the set of remainders in modulo n
- Has a finite number of values, and loops back from either end
- Modular arithmetic
  - Can perform addition and multiplication
  - Do modulo to reduce the answer to the finite set
- Can do reduction at any point, ie
  - `a+b mod n = a mod n + b mod n`

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

Properties of Modular Arithmetic in Z_n

$Z_n = \{0, 1, \ldots, n-1\}$

- Commutative laws
  $(w + x) \bmod n = (x + w) \bmod n$
  $(w \times x) \bmod n = (x \times w) \bmod n$
- Associative laws
  $[(w + x) + y] \bmod n = [w + (x + y)] \bmod n$
  $[(w \times x) \times y] \bmod n = [w \times (x \times y)] \bmod n$
- Distributive laws
  $[w + (x \times y)] \bmod n = [(w + x) \times (w + y)] \bmod n$
  $[w \times (x + y)] \bmod n = [(w \times x) + (w \times y)] \bmod n$
- Identities
  $(0 + w) \bmod n = w \bmod n$
  $(1 \times w) \bmod n = w \bmod n$
- Additive inverse (-w)
  For each $w \in Z_n$, there exists a z such that $w + z \equiv 0 \bmod n$
- Form a commutative ring for addition with an additive identity

Modular Arithematic- Example

1. [(a mod n) + (b mod n)] mod n = (a + b) mod n

   [(11 mod 8) + (15 mod 8)] mod 8 = 10 mod 8 = 2 (11 + 15) mod 8 = 26 mod 8 = 2

2. [(a mod n) – (b mod n)] mod n = (a – b) mod n

   [(11 mod 8) – (15 mod 8)] mod 8 = –4 mod 8 = 4 (11 – 15) mod 8 = –4 mod 8 = 4

3. [(a mod n) x (b mod n)] mod n = (a x b) mod n

   [(11 mod 8) x (15 mod 8)] mod 8 = 21 mod 8 = 5 (11 x 15) mod 8 = 165 mod 8 = 5

Addition mod 8 Example

- $Z_8 = \{0, 1, \ldots, 7\}$

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

Multiplication mod 8

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

- When you multiply 2 with every element of Z_8, you do not get eight distinct answers. (Multiplying 2 with every element of Z_8 yields {0, 2, 4, 6, 0, 2, 4, 6} that has only four distinct elements)

Arithmetic on Z_n

- Additive and multiplicative inverse mod 8
- Z_8 is not a finite field because it does not contain a unique multiplicative inverse for every non-zero element.
- $2 \times 4 = 0$, which is a clear violation of the M6 rule for integral domains.
- $Z_n = \{0,1,...,n-1\}$ is not an **integral domain**
- Multiplicative inverses exist for only those elements of Z_n that are relatively prime to n

w	$-w$	w^{-1}
0	0	—
1	7	1
2	6	—
3	5	3
4	4	—
5	3	5
6	2	—
7	1	7

Prime Finite Fields

- An element a of Z_n does not have a multiplicative inverse if a is not relatively prime to the modulus n
- What if we choose the modulus n to be a prime number? (A prime number has only two divisors, one and itself)
- For a prime n, every non-zero element $a \in Z_n$ will be relatively prime to n.
- That implies that there will exist a multiplicative inverse for every non-zero $a \in Z_n$ for prime n

Example Z_7

- Multiplication mod 7

×	0	1	2	3	4	5	6
0	0	0	0	0	0	0	0
1	0	1	2	3	4	5	6
2	0	2	4	6	1	3	5
3	0	3	6	2	5	1	4
4	0	4	1	5	2	6	3
5	0	5	3	1	6	4	2
6	0	6	5	4	3	2	1

- Multiplicative inv mod 7

1	2	3	4	5	6
2	4	6	(1)	3	5
3	6	2	5	(1)	4
4	(1)	5	2	6	3
5	3	(1)	6	4	2
6	5	4	3	2	(1)

,

Prime Finite Fields

- Whether Z_p guarantee an integral domain: M6: no zero divisors (ab=0 means either a=0 or b=0)?
- $a \times b = 0$ for general Z_n occurs only when non-zero a and b are factors of the modulus n.
- When n is a prime, its only factors are 1 and n.
- So, with the elements of Z_n being in the range 0 through $n - 1$, the only time we will see $a \times b = 0$ is when either a is 0 or b is 0.
- Hence, Z_p obeys M6 also
- Z_p obeys all A1-A5 and M1-M7 as well as finite
- Hence known as Prime Finite Fields

Galois Fields GF(p)

- Z_p is a finite field if p is a prime number.
- Z_p is sometimes referred to as a prime finite field.
- Such a field is also denoted GF(p), where GF stands for "Galois Field"
- We are interested in two finite fields of *p*, where *p* is prime,
  - GF(*p*)
  - GF(p^n)
    - n = 1 is called prime field
    - n > 1 is called an extension field

Polynomial Arithmetic

- We can represent a bit pattern by a polynomial, say with the variable x
- Each power of x in the polynomial can stand for a bit position in a bit pattern
- Example, can represent the bit pattern
  - 111 by the polynomial $x^2 + x + 1$
  - 101 by the polynomial $x^2 + 1$
  - 011 by the polynomial $x + 1$
- Representing a bit pattern with a polynomial will allow us to create a finite field with bit patterns

Polynomial Arithmetic

- In general, a polynomial is an expression of the form

$$f(x) = a_n x^n + a_{n-1} x^{n-1} + \cdots + a_1 x + a_0 = \sum_{i=0}^{n} a_i x^i$$

  For some non-negative integer n and where the coefficients a_0, a_1, ..., a_n are drawn from some designated set S, called the coefficient set
- When $a_n \neq 0$, we have a polynomial of degree n
- Polynomial arithmetic deals with addition, subtraction, multiplication, and division of polynomials.

Ordinary Polynomial Arithmetic

- Add or subtract corresponding coefficients
- Multiply all terms by each other
- eg

$$f(x) = a_2x^2 + a_1x + a_0 \quad g(x) = b_1x + b_0$$

$$f(x) + g(x) = a_2x^2 + (a_1 + b_1)x + (a_0 + b_0)$$

$$f(x) - g(x) = -b_3x^3 + a_2x^2 + a_1x + (a_0 - b_0)$$

$$f(x) \times g(x) = a_2b_1x^3 + (a_2b_0 + a_1b_1)x^2 + (a_1b_0 + a_0b_1)x + a_0b_0$$

$$\frac{8x^2 + 3x + 2}{2x + 1} = 4x - 0.5 + \frac{2.5}{2x + 1}$$

Polynomial Arithmetic

- Several alternatives available
  - Ordinary polynomial arithmetic
  - Poly arithmetic with coefficients mod p
  - Poly arithmetic with coefficients mod p and polynomials mod another polynomial M(x)
- With n points, we define a unique n-1 degree polynomial, and the polynomial behaves nicely as fields by obeying the 12 axioms.
- We can use polynomials to model Shift and XOR operations (used in AES)
- So we can do all the operations we need for secret sharing using polynomials

Polynomial Arithmetic with *mod* Coefficients

- When computing the value of each coefficient, modulo some value could be modulo with any prime
- Modulo arithmetic on a polynomial with GF(7)
- 7 has additive Inverse and multiplicative Inverse

Z_7:	0	1	2	3	4	5	6
AI:	0	6	5	4	3	2	1
MI:	–	1	4	5	2	3	6

Polynomial Arithmetic with GF(7): Example

$$f(x) = 5x^2 + 4x + 6 \qquad g(x) = 2x + 1$$

$$f(x) + g(x) = 5x^2 + 6x$$

$$f(x) - g(x) = 5x^2 + 2x + 5$$

$$f(x) \times g(x) = 3x^3 + 6x^2 + 2x + 6$$

Division of Polynomials in GF(7)

divide $5x^2 + 4x + 6$ by $2x + 1$

Z_7:	0	1	2	3	4	5	6
AI:	0	6	5	4	3	2	1
MI:	–	1	4	5	2	3	6

$6x + 6$

$2x + 1 \;\overline{)\; 5x^2 + 4x + 6}$

$5x^2 + 6x$

$-2x + 6$

$5x + 6$

0

$\frac{5x^2}{2x} = 6x$

$-2 \bmod 7 = 5$

$\frac{5}{2} = 6$

$5 \times 2^{-1} = 20 \bmod 7 = 6$

$f(x) \;/\; g(x) \quad = \quad 6x + 6$

Modular Polynomial Arithmetic

- Given any polynomials f and g, can write in the form:
  - $f(x) = q(x)\, g(x) + r(x)$
  - can interpret $r(x)$ as being a remainder
  - $r(x) = f(x) \bmod g(x)$
- If have no remainder, then say $g(x)$ divides $f(x)$
- If $g(x)$ has no divisors other than itself and 1, say it is **irreducible** (or **prime**) polynomial
- **Modular polynomial arithmetic modulo an irreducible polynomial forms a field**
  - Polynomials can model Shift and XOR operations for cryptography operations purpose

Polynomials Over GF(2)

- GF(2) consists of the set {0, 1}
- Example Polynomials

$$x^3 + x^2 + 1$$
$$x^5 + x^4 + x^2 + 1$$
$$x + 1$$

- Addition over GF(2) is equivalent to the logical XOR

$$0 + 0 = 0$$
$$0 + 1 = 1$$
$$1 + 0 = 1$$
$$1 + 1 = 0$$

- Multiplication to the logical AND operation

$$0 \times 0 = 0$$
$$0 \times 1 = 0$$
$$1 \times 0 = 0$$
$$1 \times 1 = 1$$

Polynomials Arithmetic Over GF(2)

$$f(x) = x^2 + x + 1$$

$$g(x) = x + 1$$

$$f(x) + g(x) = x^2$$

$$f(x) - g(x) = x^2$$

$$f(x) \times g(x) = x^3 + 1$$

$$f(x) \,/\, g(x) = x + \frac{1}{x+1}$$

$$\begin{array}{r|l} & x \\ x+1 & x^2+x+1 \\ & x^2+x \\ \hline & 1 \end{array}$$

Polynomial GCD

- To find the greatest common divisor for polynomials
- GCD: the one with the greatest degree
  - *c(x)* = GCD(*a(x), b(x)*) if *c(x)* is the poly of greatest degree which divides both *a(x), b(x)*
  - can adapt Euclid's Algorithm to find it:
  - EUCLID[*a*(*x*), *b*(*x*)]

1. A(*x*) = *a*(*x*); B(*x*) = *b*(*x*)
2. **if** B(*x*) = 0 **return** A(*x*) = gcd[*a*(*x*), *b*(*x*)]
3. R(*x*) = A(*x*) mod B(*x*)
4. A(*x*) = B(*x*)
5. B(*x*) = R(*x*)
6. **goto** 2

Polynomial GCD Example

$$gcd(b_1, b_2) = gcd(b_2, b_1 \bmod b_2) = gcd(b_2, b_3)$$
$$= gcd(b_3, b_2 \bmod b_3) = gcd(b_3, b_4)$$
$$= gcd(b_4, b_3 \bmod b_4) = gcd(b_4, b_5)$$
$$\ldots\ldots \qquad \ldots\ldots$$
$$\ldots\ldots \qquad \ldots\ldots$$
$$gcd(b_{m-1}, b_m)$$

until b_m is either 0 or 1.

$$a(x) = 6x^4 + 2x^3 + 5x^2 + 3x + 2, \qquad b(x) = 2x^2 + 1$$

$= gcd(2x^2+1,\ 6x^4+2x^3+5x^2+3x+2)$

$$\begin{array}{r|l} & 3x^2 + x + 1 \\ \hline 2x^2+1 & 6x^4 + 2x^3 + 5x^2 + 3x + 2 \\ & 6x^4 \qquad\quad + 3x^2 \\ \hline & 2x^3 + 2x^2 + 3x + 2 \\ & 2x^3 \qquad\quad + x \\ \hline & 2x^2 + 2x + 2 \\ & 2x^2 \qquad\quad + 1 \\ \hline & 2x + 1 \end{array}$$

$$a(x) = (3x^2+x+1)\, b(x) + r_1(x) \text{ where } r_1(x) = 2x+1$$

Polynomial GCD Example

$$a(x) = (3x^2+x+1)(2x^2+1)+ r_1(x) \text{ where } r_1(x) = 2x+1$$

$$= \gcd(2x^2+1,\ 2x+1)$$

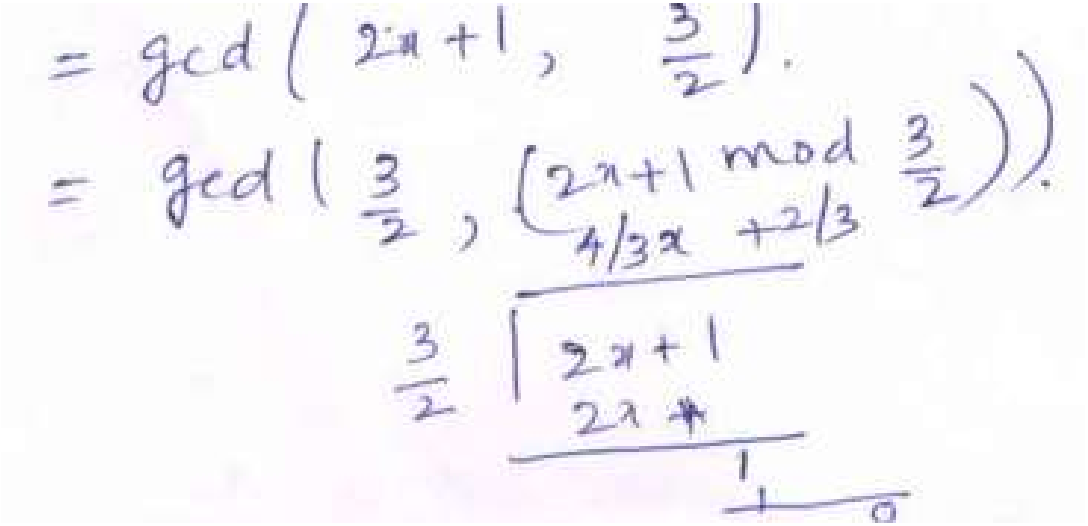
$$b(x) = (x-\tfrac{1}{2})\, r_1(x) + r_2(x) \text{ where } r_2(x) = \tfrac{3}{2}$$

$$= \gcd(2x+1,\ 2x^2+1)$$

$$\begin{array}{r|l} & x - \frac{1}{2} \\ \hline 2x+1 & 2x^2+1 \\ & 2x^2+x \\ \hline & -x+1 \\ & -x-\frac{1}{2} \\ \hline & \frac{3}{2} \end{array}$$

Polynomial GCD Example

$$b(x) = (x-\tfrac{1}{2})\, r_1(x) + r_2(x) \text{ where } r_2(x) = \tfrac{3}{2}$$

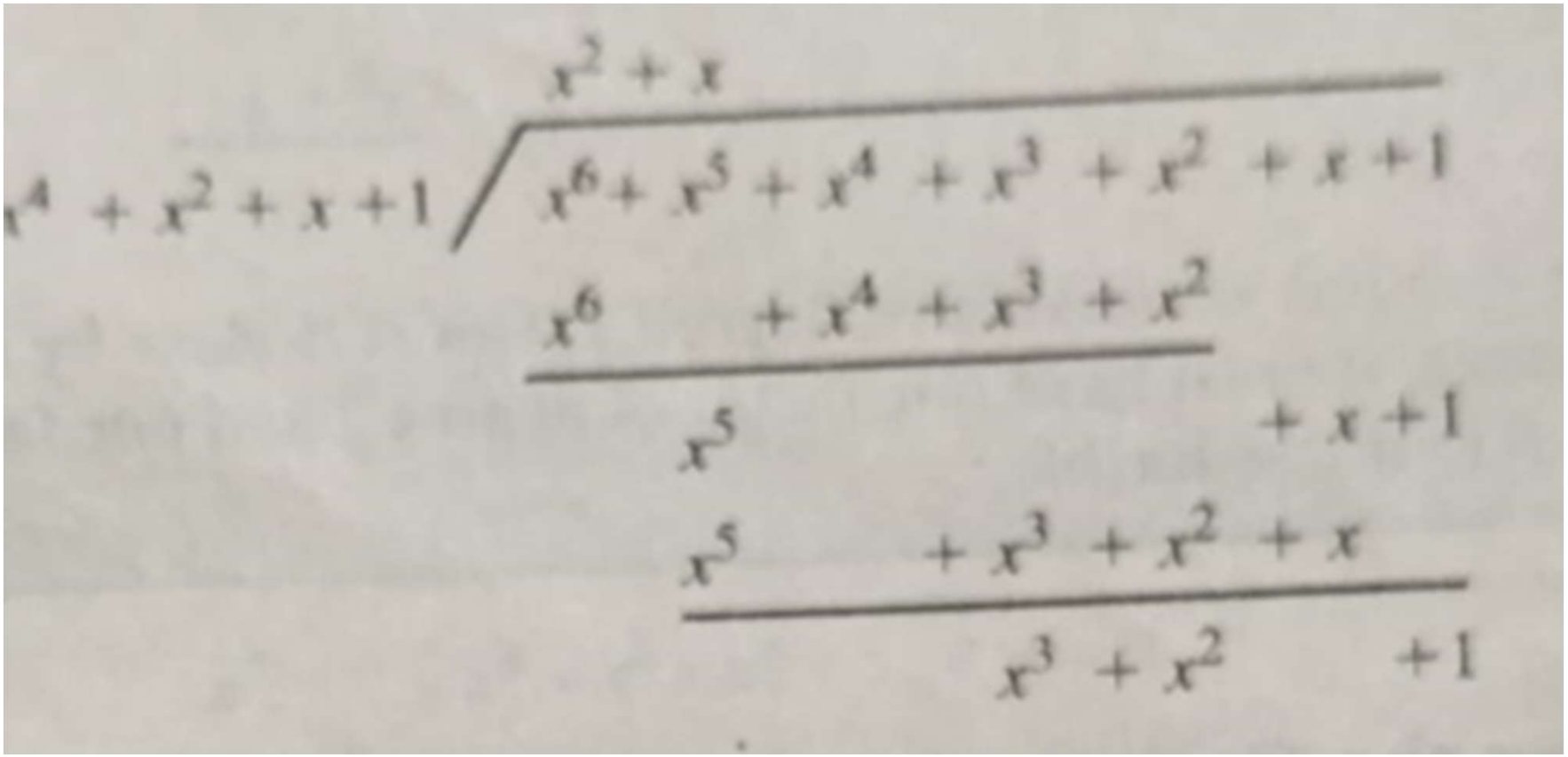


$$r_1(x) = (\tfrac{4}{3}x+\tfrac{2}{3})\, r_2(x) + 0$$

gcd is the last non-zero remainder: $d(x) = r_2(x) = \tfrac{3}{2}$

Example 2

- Find GCD ($x^6+x^5+x^4+x^3+x^2+x+1$, x^4+x^2+x+1) in GF(2)



Example 2

$$
\begin{array}{r}
x+1 \\
x^3+x^2+1 \;\overline{)\; x^4 + x^2 + x + 1} \\
\underline{x^4 + x^3 \quad + x} \\
x^3 + x^2 + 1 \\
\underline{x^3 + x^2 + 1} \\
0
\end{array}
$$

$$R(x) = A(x) \bmod B(x) = 0$$

$$\gcd[a(x), b(x)] = A(x) = x^3 + x^2 + 1$$

When is Polynomial Division Permitted?

- Polynomial division is obviously not allowed for polynomials that are not defined over fields.
- Example, for polynomials defined over the set of all integers, you cannot divide $4x^2 + 5$ by the polynomial $5x$.
  - If you tried, the first term of the quotient would be $(4/5)x$ where the coefficient of x is not an integer

Prime Polynomial

- When g(x) divides f(x) without leaving a remainder, we say g(x) is a factor of f(x)
- A polynomial f(x) over a field F is called irreducible if f(x) cannot be expressed as a product of two polynomials, both over F and both of degree lower than that of f(x)
- An irreducible polynomial is also referred to as a prime polynomial.
- Examples: over GF(2): $x^3 + x + 1$ and $x^3 + x^2 + 1$

Example

- 1 + 1 = 0 in GF(2).

$$
\begin{aligned}
&\left((x^2 + x + 1) \times (x^2 + 1)\right) \ mod \ (x^3 + x + 1) \\
&= \left((x^4 + x^3 + x^2) + (x^2 + x + 1)\right) \ mod \ (x^3 + x + 1) \\
&= \left(x^4 + x^3 + x + 1\right) \ mod \ (x^3 + x + 1) \\
&= -x^2 - x \\
&= x^2 + x
\end{aligned}
$$

Polynomials over GF(2^3)

- With multiplications modulo $x^3 + x + 1$, have only eight polynomials in the set of polynomials over GF(2):
  - 0
  - 1
  - x
  - x^2
  - x + 1
  - $x^2 + 1$
  - $x^2 + x$
  - $x^2 + x + 1$
- Will refer to this set as GF(2^3) where the exponent of 2, which in this case is **3**, is the **degree of the modulus polynomial**

Modular Polynomial Arithmetic

- Can compute in field GF(2^n)
  - Polynomials with coefficients modulo 2
  - Whose degree is less than n
  - Coefficients always modulo 2 in an operation
  - hence must modulo an irreducible polynomial of degree n (for multiplication only)
- Form a finite field
- Can always find an inverse
  - can use Extended Euclid's Inverse algorithm to find

$GF(2^3)$ and Z_8

- Conceptualization of $GF(2^3)$ is analogous to conceptualization of the set Z_8.
- Eight elements of Z_8 are to be thought of as integers modulo 8
- Basically, Z_8 maps all integers to the eight numbers in the set Z_8
- Similarly, $GF(2^3)$ maps all of the polynomials over GF(2) to the eight polynomials
- But, $GF(2^3)$ is a field, whereas Z_8 is NOT.

Example GF(2^3)

Table 4.6 Polynomial Arithmetic Modulo ($x^3 + x + 1$)

	+	000 0	001 1	010 x	011 $x+1$	100 x^2	101 x^2+1	110 x^2+x	111 x^2+x+1
000	0	0	1	x	$x+1$	x^2	x^2+1	x^2+x	x^2+x+1
001	1	1	0	$x+1$	x	x^2+1	x^2	x^2+x+1	x^2+x
010	x	x	$x+1$	0	1	x^2+x	x^2+x+1	x^2	x^2+1
011	$x+1$	$x+1$	x	1	0	x^2+x+1	x^2+x	x^2+1	x^2
100	x^2	x^2	x^2+1	x^2+x	x^2+x+1	0	1	x	$x+1$
101	x^2+1	x^2+1	x^2	x^2+x+1	x^2+x	1	0	$x+1$	x
110	x^2+x	x^2+x	x^2+x+1	x^2	x^2+1	x	$x+1$	0	1
111	x^2+x+1	x^2+x+1	x^2+x	x^2+1	x^2	$x+1$	x	1	0

(a) Addition

	×	000 0	001 1	010 x	011 $x+1$	100 x^2	101 x^2+1	110 x^2+x	111 x^2+x+1
000	0	0	0	0	0	0	0	0	0
001	1	0	1	x	$x+1$	x^2	x^2+1	x^2+x	x^2+x+1
010	x	0	x	x^2	x^2+x	$x+1$	1	x^2+x+1	x^2+1
011	$x+1$	0	$x+1$	x^2+x	x^2+1	x^2+x+1	x^2	1	x
100	x^2	0	x^2	$x+1$	x^2+x+1	x^2+x	x	x^2+1	1
101	x^2+1	0	x^2+1	1	x^2	x	x^2+x+1	$x+1$	x^2+x
110	x^2+x	0	x^2+x	x^2+x+1	1	x^2+1	$x+1$	x	x^2
111	x^2+x+1	0	x^2+x+1	x^2+1	x	1	x^2+x	x^2	$x+1$

(b) Multiplication

GF of AES

- GF(2^n) is a Finite Field for every n
- AES arithmetic is based on GF(2^8), which uses the irreducible polynomial $x^8 + x^4 + x^3 + x + 1$
- AES contains 256 distinct polynomials over GF(2)
- Since coefficients are 0 or 1, can represent any such polynomial as a bit string
- Ex. GF(2^8), 10001101 as $x^7 + x^3 + x^2 + 1$

Addition Operation

- Given any n, can come up with 2^n bit patterns
- n bits form a set of integers that would constitute a finite field only if there is an irreducible polynomial of degree n is available
- Addition becomes XOR of these bit strings
- Ex: 2^8

$$
\begin{aligned}
5 + 13 &= 0000\,0101 + 0000\,1101 = 0000\,1000 = 8 \\
76 + 22 &= 0100\,1100 + 0001\,0110 = 0101\,1010 = 90 \\
7 - 3 &= 0000\,0111 - 0000\,0011 = 0000\,0100 = 4 \\
7 + 3 &= 0000\,0111 + 0000\,0011 = 0000\,0100 = 4
\end{aligned}
$$

Multiplication in the AES field

- Given two polynomials a(x) and b(x) in GF(2^8), their product will be a(x) x b(x) mod m(x) and we immediately reduce all coefficients mod 2
- If the result is a polynomial of degree 8 or greater, reduce to result mod $x^8 + x^4 + x^3 + x + 1$
- Ex:

$$(x^4 + x^3 + x)(x^3 + x^2 + 1)$$

$$= x^7 + x^6 + x^5 + x^6 + x^5 + x^4 + x^4 + x^3 + x^2$$
$$= x^7 + 2x^6 + 2x^5 + 2x^4 + x^3 + x^2$$
$$= x^7 + x^3 + x^2$$

Multiplication Example

$$(x^6 + x)(x^4+1)$$

$$(x^{10} + x^7 + x^5 + x) \bmod (x^8 + x^4 + x^3 + x + 1)$$

$$\begin{array}{r|l} & 1 \\ \hline 100011011 & 100101000 10 \\ & 100011011 \\ \hline & 11001110 \end{array}$$

$$= x^7 + x^6 + x^3 + x^2 + x$$

Multiplying a General Polynomial in GF(2^8)

- Let $f(x) = b_7x^7+b_6x^6+b_5x^5+b_4x^4+b_3x^3+b_2x^2+b_1x+b_0$
- Bit pattern of f(x) is $b_7b_6b_5b_4b_3b_2b_1b_0$
- $f(x)\times x = b_7x^8+b_6x^7+b_5x^6+b_4x^5+b_3x^4+b_2x^3+b_1x^2+b_0x$
- To find $f(x)\times x \bmod x^8+x^4+x^3+x+1$ (multiply by 2)
- If the bit b_7 of f(x) is equals 0
  - then the result is $b_6x^6+b_5x^5+b_4x^4+b_3x^3+b_2x^2+b_1x+b_0$ and nothing further needs to be done.
  - Output bit pattern is $b_6b_5b_4b_3b_2b_1b_0$
  - Example f(x),x = 01010111 X 00000010 = 10101110
  - Nothing but a 1- bit left shift

Multiplying a General Polynomial in GF(2^8)

- If the bit b_7 of f(x) is equals 1
  - $(b_7x^8+b_6x^7+b_5x^6+b_4x^5+b_3x^4+b_2x^3+b_1x^2+b_0x)$ mod $(x^8+x^4+x^3+x+1)$

$= b_6x^7+b_5x^6+b_4x^5+b_3x^4+b_2x^3+b_1x^2+b_0x + x^4+x^3+x+1$

$= (b_6b_5b_4b_3b_2b_1b_0) \otimes (00011011)$

Example:

f(x) = 10101110, f(x).x = 10101110 x 00000010 = 101011100 mod 100011011 = 01000111

- A 1- bit left shift followed by a conditional XOR with (0001 1011)
- LS, $\otimes$ = 01011100 $\otimes$ 00011011 = 01000111

Multiplying a General Polynomial in GF(2^8)

- to multiply two bit patterns B1 and B2, each 8 bits long
- If B2 is the bit pattern 00000001, then the result is B1 itself.
- If B2 is the bit pattern 00000010, then it is multiplying B1 by x
  - If the MSB bit in B1 is 0, the result is obtained by shifting the B1 bit pattern to the left by one bit and inserting a 0 bit from the right.
  - If B1's MSB is 1, first shift the B1 bit pattern to the left and then take its XOR with the bit pattern 00011011 (x^4+x^3+x+1)

Multiplying a General Polynomial in GF(2^8)

- If B2 is the bit pattern 00000100, then we are multiplying B1 by x^2 .
  - This amounts to first multiplying B1 by x, and then multiplying the result again by x.
  - So it amounts to two times applications of the logic in the case of multiplying with x
- In general, if B2 consists of a single bit in the j^{th} position from the right, needs j applications of the logic laid out for multiplying with x.
- Even more generally, when B2 consists of an arbitrary bit pattern, consider the bit pattern to be a sum of bit patterns each containing only single bit

Example

- $f(x) = x^6 + x^4 + x^2 + x + 1$ (01010111)

  $g(x) = x^7 + x + 1$ (10000011) and

  $m(x) = x^8 + x^4 + x^3 + x + 1$ (100011011)

To find f(x).g(x) mod m(x)

Multiplying a General Polynomial in GF(2^8)

- If B2 is 10000011,
- B1 × 10000011 = B1 × (00000001 + 00000010 + 10000000)
- = (B1 × 00000001) + (B1 × 00000010) + (B1 × 10000000)
- = (B1 × 00000001) ⊗ (B1 × 00000010) ⊗ (B1 × 10000000)
- Each of the three multiplications shown in the final expression involves the logic of multiplying B1 with a single power of x

Example

- f(x).x = (01010111) * (00000010) = (10101110) //SL
- f(x).x^2 = (01010111) * (00000100) = (01011100) ⊕ (00011011) = (01000111)
- f(x).x^3 = (01010111) * (00001000) = (10001110)
- f(x).x^4 = (01010111) * (00010000) = (00011100) ⊕ (00011011) = (00000111)
- f(x).x^5 = (01010111) * (00100000) = (00001110)
- f(x).x^6 = (01010111) * (01000000) = (00011100)
- f(x).x^7 = (01010111) * (10000000) = (00111000)
- 01010111) * (10000011) = (01010111) * [(00000001) ⊕ (00000010) ⊕ (10000000)]
- = (01010111) ⊕ (10101110) ⊕ (00111000) = (11000001) = x7 + x6 + 1

Multiplicative Inverses in GF(2^n)

- Can division be carried out directly on the bit patterns?
- Can do if you knew the multiplicative inverses of the bit patterns
- can use the Extended Euclid's Algorithm, provided you carry out all the arithmetic in that algorithm according to the rules appropriate for GF(2^n).
- Example: for GF(2^3).

	Additive Inverse	Multiplicative Inverse
000	000	-----
001	001	001
010	010	101
011	011	110
100	100	111
101	101	010
110	110	011
111	111	100