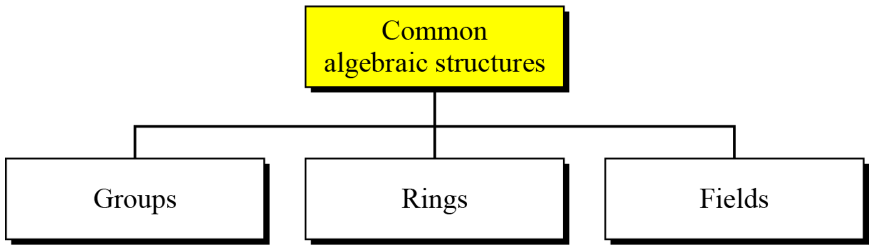
MATHEMATICS OF CRYPTOGRAPHY
PART II
ALGEBRAIC STRUCTURES

ALGEBRAIC STRUCTURES

- Cryptography requires sets of integers and specific operations that are defined for those sets.
- The combination of the set and the operations that are applied to the elements of the set is called an algebraic structure.
- Three common algebraic structures: groups, rings, and fields.

ALGEBRAIC STRUCTURES(cont.)



Common algebraic structure

Groups

- A group (G) is a set of elements with a binary operation (•) that satisfies four properties (or axioms).
  - Closure
  - Associativity
  - Existence of identity
  - Existence of inverse

Groups(cont.)

- Closure
  - If a and b are elements of G, then c = a•b is also an element of G.
- Associativity
  - If a, b and c are elements of G, then (a•b) •c=a•(b•c)
- Existence of identity
  - For all a in G, there exist an element e, called the identity element, such that e•a=a•e=a
- Existence of inverse
  - For each a in G, there exists an element a', called the inverse of a, such that a•a'=a'•a=e

Groups(cont.)

- A Commutative group (Abelian group) is group in which the operator satisfies four properties plus an extra property that is commutativity.
  - For all a and b in G, we have a • b = b • a

Groups(cont.)

- Example

  The set of residue integers with the addition operator,

  $$G = < Z_n , +>,$$

  is a commutative group.

  Check the properties.....

Groups(cont.)

- Example:
  - The set Z_n^* with the multiplication operator, G = $<Z_n^*, \times>$, is also an abelian group.
- Example:
  - Let us define a set G = < {a, b, c, d}, •> and the operation as shown in Table.

•	a	b	c	d
a	a	b	c	d
b	b	c	d	a
c	c	d	a	b
d	d	a	b	c

Groups(cont.)

- Example:
  - A very interesting group is the permutation group.
  - The set is the set of all permutations, and the operation is composition: applying one permutation after another.
  - Check for properties….
    - Is the group abelian????

Groups(cont.)

- Example(cont.):

∘	[1 2 3]	[1 3 2]	[2 1 3]	[2 3 1]	[3 1 2]	[3 2 1]
[1 2 3]	[1 2 3]	[1 3 2]	[2 1 3]	[2 3 1]	[3 1 2]	[3 2 1]
[1 3 2]	[1 3 2]	[1 2 3]	[2 3 1]	[2 1 3]	[3 2 1]	[3 1 2]
[2 1 3]	[2 1 3]	[3 1 2]	[1 2 3]	[3 2 1]	[1 3 2]	[2 3 1]
[2 3 1]	[2 3 1]	[3 2 1]	[1 3 2]	[3 1 2]	[1 2 3]	[2 1 3]
[3 1 2]	[3 1 2]	[2 1 3]	[3 2 1]	[1 2 3]	[2 3 1]	[1 3 2]
[3 2 1]	[3 2 1]	[2 3 1]	[3 1 2]	[1 3 2]	[2 1 3]	[1 2 3]

Operation table for permutation group

Groups(cont.)

- In the previous example, we showed that a set of permutations with the composition operation is a group.
- This implies that using two permutations one after another cannot strengthen the security of a cipher.
- Because we can always find a permutation that can do the same job because of the closure property.

Groups(cont.)

- Application
  - Although a group involves a single operation, the properties imposed on the operation allow the use of a pair of operations!!!!
  - How???

Groups(cont.)

- Finite Group
  - If the set has a finite number of elements; otherwise, it is an infinite group.
- Order of a Group |G|
  - The number of elements in the group.
  - If the group is finite, its order is finite
- Subgroups
  - A subset H of a group G is a subgroup of G if H itself is a group with respect to the operation on G

Groups(cont.)

- Subgroups(cont.)
  - If G=<S, •> is a group, H=<T, •> is a group under the same operation, and T is a nonempty subset of S, then H is a subgroup of G
    - If a and b are members of both groups, then c=a•b is also member of both groups
    - The group share the same identity element
    - If a is a member of both groups, the inverse of a is also a member of both groups
    - The group made of the identity element of G, H=<{e}, •>, is a subgroup of G
    - Each group is a subgroup of itself

Groups(cont.)

- Exercise:
  - Is the group H = <Z_{10}, +> a subgroup of the group G = <Z_{12}, +>?

Groups(cont.)

- Exercise:
  - Is the group H = <Z_{10}, +> a subgroup of the group G = <Z_{12}, +>?
- Solution:
  - The answer is no. Although H is a subset of G, the operations defined for these two groups are different. The operation in H is addition modulo 10; the operation in G is addition modulo 12.

Groups(cont.)

- Cyclic subgroups
  – If a subgroup of a group can be generated using the power of an element, the subgroup is called the cyclic subgroup.

$$\boxed{a^n \rightarrow a \bullet a \bullet \ldots \bullet a \quad (n \text{ times})}$$

Groups(cont.)

- Four cyclic subgroups can be made from the group G = <Z_6, +>.
- They are H_1 = <{0}, +>, H_2 = <{0, 2, 4}, +>, H_3 = <{0, 3}, +>, and H_4 = G.

$0^0 \bmod 6 = 0$

$1^0 \bmod 6 = 0$
$1^1 \bmod 6 = 1$
$1^2 \bmod 6 = (1 + 1) \bmod 6 = 2$
$1^3 \bmod 6 = (1 + 1 + 1) \bmod 6 = 3$
$1^4 \bmod 6 = (1 + 1 + 1 + 1) \bmod 6 = 4$
$1^5 \bmod 6 = (1 + 1 + 1 + 1 + 1) \bmod 6 = 5$

$2^0 \bmod 6 = 0$
$2^1 \bmod 6 = 2$
$2^2 \bmod 6 = (2 + 2) \bmod 6 = 4$

$3^0 \bmod 6 = 0$
$3^1 \bmod 6 = 3$

$4^0 \bmod 6 = 0$
$4^1 \bmod 6 = 4$
$4^2 \bmod 6 = (4 + 4) \bmod 6 = 2$

$5^0 \bmod 6 = 0$
$5^1 \bmod 6 = 5$
$5^2 \bmod 6 = 4$
$5^3 \bmod 6 = 3$
$5^4 \bmod 6 = 2$
$5^5 \bmod 6 = 1$

Groups(cont.)

- Exercise:
  – Find out the cyclic subgroups for group G = <Z_{10}*, ×>.

Groups(cont.)

- Three cyclic subgroups can be made from the group G = <Z_{10}*, ×>. G has only four elements: 1, 3, 7, and 9. The cyclic subgroups are H_1 = <{1}, ×>, H_2 = <{1, 9}, ×>, and H_3 = G.

$1^0 \bmod 10 = 1$

$3^0 \bmod 10 = 1$
$3^1 \bmod 10 = 3$
$3^2 \bmod 10 = 9$
$3^3 \bmod 10 = 7$

$7^0 \bmod 10 = 1$
$7^1 \bmod 10 = 7$
$7^2 \bmod 10 = 9$
$7^3 \bmod 10 = 3$

$9^0 \bmod 10 = 1$
$9^1 \bmod 10 = 9$

Groups(cont.)

- Cyclic group
  - A cyclic group is a group that is its own cyclic subgroup.

$$\boxed{\{e, g, g^2, \ldots, g^{n-1}\}, \text{ where } g^n = e}$$

Groups(cont.)

- Cyclic group(cont.)
- Example:
  - Three cyclic subgroups can be made from the group G = < $Z_{10}{}^*$, ×>.
  - The cyclic subgroups are H_1 = <{1}, ×>, H_2 = <{1, 9}, ×>, and H_3 = G.
  - The group G = <$Z_{10}{}^*$, ×> is a cyclic group with two generators, g = 3 and g = 7.
  - The group G = <Z_6, +> is a cyclic group with two generators, g = 1 and g = 5.

Groups(cont.)

- Lagrange's Theorem
  - Assume that G is a group, and H is a subgroup of G. If the order of G and H are |G| and |H|, respectively, then, based on this theorem, |H| divides |G|.
- Order of an Element
  - The order of an element is the order of the cyclic group it generates.

Groups(cont.)

- Example:
  - In the group G = $<Z_6, +>$, the orders of the elements are:

    ord(0) = 1, ord(1) = 6, ord(2) = 3, ord(3) = 2, ord(4) = 3, ord(5) = 6.

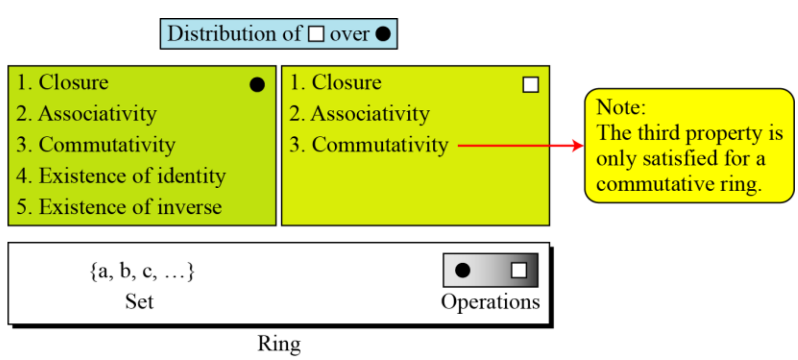
  - In the group G = $<Z_{10}^*, \times>$, the orders of the elements are: ord(1) = 1, ord(3) = 4, ord(7) = 4, ord(9) = 2.

Ring

- A ring, R = <{…}, •,■ >, is an algebraic structure with two operations.
- First operation must satisfy all five properties
- Second operation must satisfy only the first two
- In addition, second operation must be distributed over first
  - i.e. for all a, b, and c elements of R, we have,
    a■(b • c) = (a ■ b) • (a ■ c) and
    (a • b) ■ c = (a■c) • (a ■ c)

Ring(cont.)

- Commutative Ring

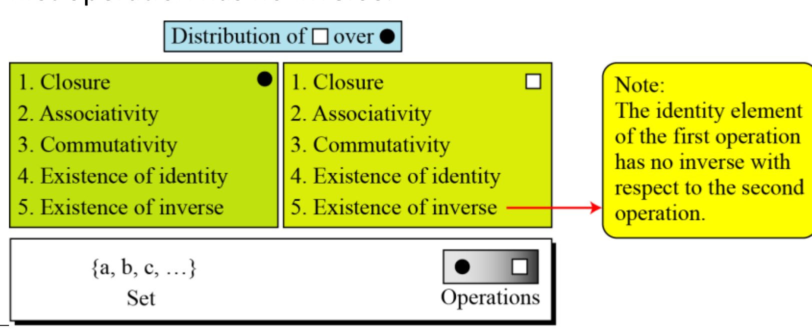


Ring(cont.)

- The set Z with two operations, addition and multiplication, is a commutative ring.
- We show it by R = <Z, +, ×>.
- Addition satisfies all of the five properties; multiplication satisfies only three properties.

Field

- A field, denoted by F = <{…}, •,■ > is a commutative ring in which the second operation satisfies all five properties defined for the first operation except that the identity of the first operation has no inverse.



Field

Field(cont.)

- Finite Fields
  - Galois showed that for a field to be finite, the number of elements should be p^n, where p is a prime and n is a positive integer.

A Galois field, GF(p^n), is a finite field with p^n elements.

Field(cont.)

- GF(p) Fields
  - When $n = 1$, we have GF(p) field.
  - This field can be the set Z_p, {0, 1, …, p − 1}, with two arithmetic operations.

Field(cont.)

- A very common field in this category is GF(2) with the set {0, 1} and two operations, addition and multiplication.

GF(2)

{0, 1} + ×

+	0	1
0	0	1
1	1	0

Addition

×	0	1
0	0	0
1	0	1

Multiplication

a	0	1
−a	1	0

a	0	1
a^{-1}	—	1

Inverses

GF(2) field

Field(cont.)

- We can define GF(5) on the set Z_5 (5 is a prime) with addition and multiplication operators.

Field(cont.)

- We can define GF(5) on the set Z_5 (5 is a prime) with addition and multiplication operators.

GF(5)

$\{0, 1, 2, 3, 4\}$ $+$ $\times$

Addition

+	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

Multiplication

×	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

Additive inverse

a	0	1	2	3	4
−a	0	4	3	2	1

Multiplicative inverse

a	0	1	2	3	4
a^{-1}	—	1	3	2	4

GF(5) field

- Summary:

Algebraic Structure	*Supported Typical Operations*	*Supported Typical Sets of Integers*
Group	$(+\ -)$ or $(\times\ \div)$	$\mathbf{Z}_n$ or $\mathbf{Z}_n{}^*$
Ring	$(+\ -)$ and $(\times)$	$\mathbf{Z}$
Field	$(+\ -)$ and $(\times\ \div)$	$\mathbf{Z}_p$

GF(2^n) FIELDS

- In cryptography, we often need to use four operations(addition, subtraction, multiplication and division).
- In other words, we need to use fields.
- However, when we work with computers, the positive integers are stored in the computers as n-bit words in which n is usually 8,16,32 and so on.
- Range of integers is 0 to $2^n – 1$
- Hence modulus is ?????
- What if we want to use field????

GF(2^n) FIELDS (cont.)

- Solution 1
  - Use GF(p), with the set Zp, where p is the largest prime number less than 2^n
  - But the problem ???
- Solution 2
  - Use GF(2^n)
  - Use a set of 2^n words
  - The elements in this set are n-bit words
  - E.g. for n=3, the set is {000,001,010,011,100,101,110,111}

GF(2^n) FIELDS (cont.)

- Solution 2
  - But the problem???

GF(2^n) FIELDS (cont.)

- Solution 2
  - But the problem???
  - 2^n is not prime
  - Need to define operations on the set of elements in GF(2^n)

GF(2^n) FIELDS (cont.)

- Let us define a GF(2^2) field in which the set has four 2-bit words: {00, 01, 10, 11}.
- We can redefine addition and multiplication for this field in such a way that all properties of these operations are satisfied.

Addition

⊕	00	01	10	11
00	00	01	10	11
01	01	00	11	10
10	10	11	00	01
11	11	10	01	00

Identity: 00

Multiplication

⊗	00	01	10	11
00	00	00	00	00
01	00	01	10	11
10	00	10	11	01
11	00	11	01	10

Identity: 01

An example of GF(2^2) field

Polynomials

- A polynomial of degree n − 1 is an expression of the form

$$f(x) = a_{n-1}x^{n-1} + a_{n-2}x^{n-2} + \cdots + a_1x^1 + a_0x^0$$

- where x^i is called the ith term and a_i is called coefficient of the *i*th term.

Polynomials (cont.)

- We can represent the 8-bit word (10011001) using a polynomial.

n-bit word	1	0	0	1	1	0	0	1

Polynomial: $1x^7 + 0x^6 + 0x^5 + 1x^4 + 1x^3 + 0x^2 + 0x^1 + 1x^0$

First simplification: $1x^7 + 1x^4 + 1x^3 + 1x^0$

Second simplification: $x^7 + x^4 + x^3 + 1$

Polynomials (cont.)

- Find the 8-bit word related to the polynomial $x^5 + x^2 + x$, we first supply the omitted terms.
- Since $n = 8$, it means the polynomial is of degree 7. The expanded polynomial is,

$$0x^7 + 0x^6 + 1x^5 + 0x^4 + 0x^3 + 1x^2 + 1x^1 + 0x^0$$

- This is related to the 8-bit word 00100110.

Polynomials (cont.)

- Operations on polynomials
  - Actually involves two operations
    - Operation on coefficients and operation on polynomials
  - Hence, need to define two fields
  - What for coefficient??
  - What for polynomials???

Polynomials (cont.)

- Operations on polynomials
  - Actually involves two operations
    - Operation on coefficients and operation on polynomials
  - Hence, need to define two fields
  - What for coefficient??
  - What for polynomials???

  - GF(2) and GF(2^n) is the answer….

Polynomials (cont.)

- Modulus
  - For the sets of polynomials in GF(2^n), a group of polynomials of degree *n* is defined as the modulus.
  - Such polynomials are referred to as irreducible polynomials.

Polynomials (cont.)

- irreducible polynomials.
  - No polynomial in the set can divide this polynomial
  - Can not be factored into a polynomial with degree of less than n

Degree	Irreducible Polynomials
1	$(x + 1)$, (x)
2	$(x^2 + x + 1)$
3	$(x^3 + x^2 + 1)$, $(x^3 + x + 1)$
4	$(x^4 + x^3 + x^2 + x + 1)$, $(x^4 + x^3 + 1)$, $(x^4 + x + 1)$
5	$(x^5 + x^2 + 1)$, $(x^5 + x^3 + x^2 + x + 1)$, $(x^5 + x^4 + x^3 + x + 1)$, $(x^5 + x^4 + x^3 + x^2 + 1)$, $(x^5 + x^4 + x^2 + x + 1)$

Polynomials (cont.)

- Polynomial addition

Addition and subtraction operations on polynomials are the same operation.

Polynomials (cont.)

- Example
- Let us do $(x^5 + x^2 + x) \oplus (x^3 + x^2 + 1)$ in $GF(2^8)$. We use the symbol $\oplus$ to show that we mean polynomial addition. The following shows the procedure:

$$
\begin{array}{l}
0x^7 + 0x^6 + 1x^5 + 0x^4 + 0x^3 + 1x^2 + 1x^1 + 0x^0 \quad \oplus \\
0x^7 + 0x^6 + 0x^5 + 0x^4 + 1x^3 + 1x^2 + 0x^1 + 1x^0 \\
\text{---} \\
0x^7 + 0x^6 + 1x^5 + 0x^4 + 1x^3 + 0x^2 + 1x^1 + 1x^0 \quad \rightarrow \quad x^5 + x^3 + x + 1
\end{array}
$$

Polynomials (cont.)

- Short cut method
  - Addition in GF(2) means the exclusive-or (XOR) operation.
  - So we can exclusive-or the two words, bits by bits, to get the result.
  - In the previous example, $x^5 + x^2 + x$ is 00100110 and $x^3 + x^2 + 1$ is 00001101.
  - The result is 00101011 or in polynomial notation $x^5 + x^3 + x + 1$.

Polynomials (cont.)

- Multiplication
  - The coefficient multiplication is done in GF(2).
  - The multiplying x^i by x^j results in x^{i+j}.
  - The multiplication may create terms with degree more than $n - 1$, which means the result needs to be reduced using a modulus polynomial.

Polynomials (cont.)

- Example
  - Find the result of $(x^5 + x^2 + x) \otimes (x^7 + x^4 + x^3 + x^2 + x)$ in $GF(2^8)$ with irreducible polynomial $(x^8 + x^4 + x^3 + x + 1)$.

$$P_1 \otimes P_2 = x^5(x^7 + x^4 + x^3 + x^2 + x) + x^2(x^7 + x^4 + x^3 + x^2 + x) + x(x^7 + x^4 + x^3 + x^2 + x)$$
$$P_1 \otimes P_2 = x^{12} + x^9 + x^8 + x^7 + x^6 + x^9 + x^6 + x^5 + x^4 + x^3 + x^8 + x^5 + x^4 + x^3 + x^2$$
$$P_1 \otimes P_2 = (x^{12} + x^7 + x^2) \bmod (x^8 + x^4 + x^3 + x + 1) = x^5 + x^3 + x^2 + x + 1$$

  - To find the final result, divide the polynomial of degree 12 by the polynomial of degree 8 (the modulus) and keep only the remainder.

Polynomials (cont.)

- Polynomial division with coefficients in GF(2)

$$x^4 + 1$$
$$x^8 + x^4 + x^3 + x + 1 \;\overline{\big)\; x^{12} + x^7 + x^2}$$
$$x^{12} + x^8 + x^7 + x^5 + x^4$$
$$\overline{x^8 + x^5 + x^4 + x^2}$$
$$x^8 + x^4 + x^3 + x + 1$$

Remainder $\boxed{x^5 + x^3 + x^2 + x + 1}$

Polynomials (cont.)

- Example:
  - In GF (2^4), find the inverse of (x^2 + 1) modulo (x^4 + x + 1).
- Solution
  - The answer is (x^3 + x + 1)

q	r_1	r_2	r	t_1	t_2	t
$(x^2 + 1)$	$(x^4 + x + 1)$	$(x^2 + 1)$	(x)	(0)	(1)	$(x^2 + 1)$
(x)	$(x^2 + 1)$	(x)	(1)	(1)	$(x^2 + 1)$	$(x^3 + x + 1)$
(x)	(x)	(1)	(0)	$(x^2 + 1)$	$(x^3 + x + 1)$	(0)
	(1)	(0)		$(x^3 + x + 1)$	(0)	

Polynomials (cont.)

- Example:
  - In GF(2^8), find the inverse of (x^5) modulo (x^8 + x^4 + x^3 + x + 1).

Polynomials (cont.)

- Example:
  - In GF(2^8), find the inverse of (x^5) modulo ($x^8 + x^4 + x^3 + x + 1$).
- Solution

q	r_1	r_2	r	t_1	t_2	t
(x^3)	$(x^8 + x^4 + x^3 + x + 1)$	(x^5)	$(x^4 + x^3 + x + 1)$	(0)	(1)	(x^3)
$(x + 1)$	(x^5)	$(x^4 + x^3 + x + 1)$	$(x^3 + x^2 + 1)$	(1)	(x^3)	$(x^4 + x^3 + 1)$
(x)	$(x^4 + x^3 + x + 1)$	$(x^3 + x^2 + 1)$	(1)	(x^3)	$(x^4 + x^3 + 1)$	$(x^5 + x^4 + x^3 + x)$
$(x^3 + x^2 + 1)$	$(x^3 + x^2 + 1)$	(1)	(0)	$(x^4 + x^3 + 1)$	$(x^5 + x^4 + x^3 + x)$	(0)
	(1)	(0)		$(x^5 + x^4 + x^3 + x)$	(0)	

Polynomials (cont.)

- A better algorithm for polynomial multiplication:
  - Obtain the result by repeatedly multiplying a reduced polynomial by *x*.
- Example:
  - Find the result of multiplying $P_1 = (x^5 + x^2 + x)$ by $P_2 = (x^7 + x^4 + x^3 + x^2 + x)$ in GF(2^8) with irreducible polynomial ($x^8 + x^4 + x^3 + x + 1$)

Polynomials (cont.)

- Solution:
  - We first find the partial result of multiplying x^0, x^1, x^2, x^3, x^4, and x^5 by P_2. Note that although only three terms are needed, the product of $x^m \otimes P_2$ for m from 0 to 5 because each calculation depends on the previous result.

Powers	*Operation*	*New Result*	*Reduction*
$x^0 \otimes P_2$		$x^7 + x^4 + x^3 + x^2 + x$	No
$x^1 \otimes P_2$	$\boldsymbol{x} \otimes (x^7 + x^4 + x^3 + x^2 + x)$	$x^5 + x^2 + x + 1$	**Yes**
$x^2 \otimes P_2$	$\boldsymbol{x} \otimes (x^5 + x^2 + x + 1)$	$x^6 + x^3 + x^2 + x$	No
$x^3 \otimes P_2$	$\boldsymbol{x} \otimes (x^6 + x^3 + x^2 + x)$	$x^7 + x^4 + x^3 + x^2$	No
$x^4 \otimes P_2$	$\boldsymbol{x} \otimes (x^7 + x^4 + x^3 + x^2)$	$x^5 + x + 1$	**Yes**
$x^5 \otimes P_2$	$\boldsymbol{x} \otimes (x^5 + x + 1)$	$x^6 + x^2 + x$	No
$\mathbf{P_1} \times \mathbf{P_2} = (x^6 + x^2 + x) + (x^6 + x^3 + x^2 + x) + (x^5 + x^2 + x + 1) = \boldsymbol{x^5 + x^3 + x^2 + x + 1}$			

Polynomials (cont.)

- Exercise:

Find the result of multiplying $P_1 = (x^3 + x^2 + x + 1)$ by $P_2 = (x^2 + 1)$ in $GF(2^4)$ with irreducible polynomial $(x^4 + x^3 + 1)$

Multiplication using computer

We have P1 = 000100110, P2 = 10011110, modulus = 100011010 (nine bits). We show the exclusive or operation by ⊕.

Powers	*Shift-Left Operation*	*Exclusive-Or*
$x^0 \otimes P_2$		10011110
$x^1 \otimes P_2$	00111100	(00111100) ⊕ (00011010) = **00100111**
$x^2 \otimes P_2$	01001110	**01001110**
$x^3 \otimes P_2$	10011100	10011100
$x^4 \otimes P_2$	00111000	(00111000) ⊕ (00011010) = 00100011
$x^5 \otimes P_2$	01000110	**01000110**
$P_1 \otimes P_2$ = (00100111) ⊕ (01001110) ⊕ (01000110) = 00101111		

Polynomials (cont.)

- Exercise:

Find the result of multiplying (10101) by (10000) in $GF(2^5)$ using $(x^5 + x^2 + 1)$ as modulus.