Basic Concepts in Number Theory and Finite Fields

Pei-Ju (Julian) Lee

National Chung Cheng University
Information Security
pjlee@mis.ccu.edu.tw

Fall, 2016

Overview

- Divisibility and the division algorithm
- The Euclidean algorithm
- Modular arithmetic
- Groups, rings, and fields
- Finite fields of the form GF(p)
- Polynomial arithmetic
- Finite fields of the form GF(2^n)

A number of cryptographic algorithms rely on properties of finite fields
Ex.
-Advanced Encryption Standard (AES)
-Elliptic curve cryptography

Divisibility

- We say that a nonzero b divides a if $a = mb$ for some m, where a, b, and m are integers
- b: divisor, a: dividend, *and* m: quotient
- The notation $b \mid a$ is commonly used
- b divides a if there is no remainder on division

Ex. The positive divisors of 24 are 1, 2, 3, 4, 6, 8, 12, and 24
$13 \mid 182$; $-5 \mid 30$; $17 \mid 289$; $-3 \mid 33$; $17 \mid 0$

Properties of Divisibility

- If $a \mid 1$, then $a = \pm 1$
- If $a \mid b$ and $b \mid a$, then $a = \pm b$
- Any $b \neq 0$ divides 0
- If $a \mid b$ and $b \mid c$, then $a \mid c$

Ex. $11 \mid 66$ and $66 \mid 198 = 11 \mid 198$

- If $b \mid g$ and $b \mid h$, then $b \mid (mg + nh)$ for arbitrary integers m and n

Properties of Divisibility

- To see this last point, note that:
  - If $b \mid g$, then g is of the form $g = b * g_1$ for some integer g_1
  - If $b \mid h$, then h is of the form $h = b * h_1$ for some integer h_1
- So:
  - $mg + nh = mbg_1 + nbh_1 = b * (mg_1 + nh_1)$

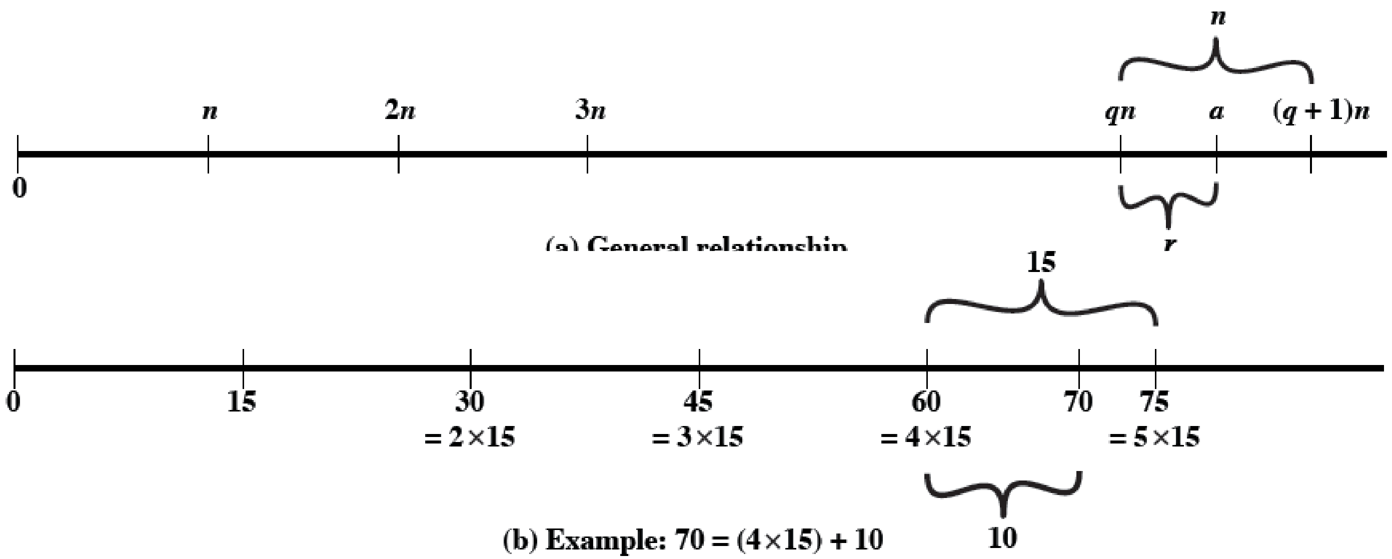
    and therefore b divides $mg + nh$

> Ex. $b = 7$; $g = 14$; $h = 63$; $m = 3$; $n = 2$
> 7 | 14 and 7 | 63.
> To show 7 (3 * 14 + 2 * 63),
> we have (3 * 14 + 2 * 63) = 7(3 * 2 + 2 * 9),
> and it is obvious that 7 | (7(3 * 2 + 2 * 9)).

Division Algorithm

- Given any positive integer *n* and any nonnegative integer *a,* if we divide *a* by *n* we get an integer quotient *q* and an integer remainder *r* that obey the following relationship:

$$a = qn + r \qquad\qquad 0 \leq r < n;\ q = [a/n]$$



Ex.
$a = 11;\ n = 7;\ \ 11 = 1 \times 7 + 4;\ \ r = 4,\ q = 1$
$a = -11;\ n = 7;\ -11 = (-2) \times 7 + 3;\ r = 3,\ q = -2$

- $-b \bmod N$
$= (-1 \cdot b) \bmod N$
$= (-1 \bmod N)\ (b \bmod N) \bmod N$
$= (N-1)\ b \bmod N$

Euclidean Algorithm

- One of the basic techniques of number theory
- Procedure for determining the greatest common divisor of two positive integers
- Two integers are relatively prime if their only common positive integer factor is 1

The first 168 prime numbers (all the prime numbers less than 1000) are:
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, 211, 223, 227, 229, 233, 239, 241, 251, 257, 263, 269, 271, 277, 281, 283, 293, 307, 311, 313, 317, 331, 337, 347, 349, 353, 359, 367, 373, 379, 383, 389, 397, 401, 409, 419, 421, 431, 433, 439, 443, 449, 457, 461, 463, 467, 479, 487, 491, 499, 503, 509, 521, 523, 541, 547, 557, 563, 569, 571, 577, 587, 593, 599, 601, 607, 613, 617, 619, 631, 641, 643, 647, 653, 659, 661, 673, 677, 683, 691, 701, 709, 719, 727, 733, 739, 743, 751, 757, 761, 769, 773, 787, 797, 809, 811, 821, 823, 827, 829, 839, 853, 857, 859, 863, 877, 881, 883, 887, 907, 911, 919, 929, 937, 941, 947, 953, 967, 971, 977, 983, 991, 997

Greatest Common Divisor (GCD)

- The greatest common divisor of *a* and *b* is the largest integer that divides both *a* and *b*
- We can use the notation gcd(a,b) to mean the greatest common divisor of *a* and *b*
- We also define gcd(0,0) = 0
- Positive integer *c* is said to be the gcd of *a* and *b* if:
  - *c* is a divisor of *a* and *b*
  - Any divisor of *a* and *b* is a divisor of *c*
- An equivalent definition is:
  - *gcd(a,b) = max[k, such that k | a and k | b]*

GCD

- Because we require that the greatest common divisor be positive,
  $gcd(a,b) = gcd(a,-b) = gcd(-a,b) = gcd(-a,-b)$
- In general, $gcd(a,b) = gcd(|a|, |b|)$

  Ex. $gcd(60, 24) = gcd(60, -24) = 12$

- Also, because all nonzero integers divide 0, we have $gcd(a,0) = |a|$
- We stated that two integers *a* and *b* are relatively prime if their only common positive integer factor is 1; this is equivalent to saying that a and b are relatively prime if $gcd(a,b) = 1$

Ex. 8 and 15 are relatively prime because the positive divisors of 8 are 1, 2, 4, and 8, and the positive divisors of 15 are 1, 3, 5, and 15. So 1 is the only integer on both lists.

Euclidean Algorithm Example

Dividend	Divisor	Quotient	Remainder
$a = 1160718174$	$b = 316258250$	$q_1 = 3$	$r_1 = 211943424$
$b = 316258250$	$r_1 = 211943424$	$q_2 = 1$	$r_2 = 104314826$
$r_1 = 211943424$	$r_2 = 104314826$	$q_3 = 2$	$r_3 = 3313772$
$r_2 = 104314826$	$r_3 = 3313772$	$q_4 = 31$	$r_4 = 1587894$
$r_3 = 3313772$	$r_4 = 1587894$	$q_5 = 2$	$r_5 = 137984$
$r_4 = 1587894$	$r_5 = 137984$	$q_6 = 11$	$r_6 = 70070$
$r_5 = 137984$	$r_6 = 70070$	$q_7 = 1$	$r_7 = 67914$
$r_6 = 70070$	$r_7 = 67914$	$q_8 = 1$	$r_8 = 2156$
$r_7 = 67914$	$r_8 = 2156$	$q_9 = 31$	$r_9 = 1078$
$r_8 = 2156$	$r_9 = 1078$	$q_{10} = 2$	$r_{10} = 0$

- Use Euclidean algorithm to find the gcd of two integers
- Ex. GCD(1160718174, 316258250) = 1078

Modular Arithmetic

- The modulus
  - If a is an integer and n is a positive integer, we define a mod n to be the remainder when a is divided by n; the integer n is called the modulus
  - thus, for any integer a:

$$a = qn + r \qquad 0 \le r < n; \; q = [a/n]$$

$$a = [a/n] * n + (a \bmod n)$$

Ex.
11 mod 7 = 4;
- 11 mod 7 = 3

Modular Arithmetic cont'd

- Congruent modulo n
  - Two integers a and b are said to be congruent modulo n if $(a \bmod n) = (b \bmod n)$
  - This is written as $a \equiv b \pmod{n}$
  - Note that if $a = 0 \pmod{n}$, then $n \mid a$

Ex.
$73 \equiv 4 \pmod{23}$;
$21 \equiv -9 \pmod{10}$

$73 \bmod 23 = 4 \bmod 23 = 4$;
$21 \bmod 10 = -9 \bmod 10 = 1$

Properties of Congruences

- Congruences have the following properties:
  1. $a \equiv b \pmod{n}$ if $n|(a - b)$
  2. $a \equiv b \pmod{n}$ implies $b \equiv a \pmod{n}$
  3. $a \equiv b \pmod{n}$ and $b \equiv c \pmod{n}$ imply $a \equiv c \pmod{n}$
- To demonstrate the first point, if $n|(a - b)$, then $(a - b) = kn$ for some k
  - So we can write $a = b + kn$
  - Therefore, (a mod n) = (remainder when $b + kn$ is divided by n) = (remainder when b is divided by n) = (b mod n)

Ex.
$23 \equiv 8 \pmod{5}$ because $23 - 8 = 15 = 5 * 3$
$-11 \equiv 5 \pmod{8}$ because $-11 - 5 = -16 = 8 * (-2)$
$81 \equiv 0 \pmod{27}$ because $81 - 0 = 81 = 27 * 3$

Modular Arithmetic

- Modular arithmetic exhibits the following properties:
  1. $[(a \text{ mod } n) + (b \text{ mod } n)] \text{ mod } n = (a + b) \text{ mod } n$
  2. $[(a \text{ mod } n) - (b \text{ mod } n)] \text{ mod } n = (a - b) \text{ mod } n$
  3. $[(a \text{ mod } n) * (b \text{ mod } n)] \text{ mod } n = (a * b) \text{ mod } n$
- We demonstrate the first property:
  - Define $(a \text{ mod } n) = r_a$ and $(b \text{ mod } n) = r_b$. Then we can write $a = r_a + jn$ for some integer j and $b = r_b + kn$ for some integer k. *Then*
  - $(a + b) \text{ mod } n = (r_a + j_n + r_b + kn) \text{ mod } n = (r_a + r_b + (k + j)n) \text{ mod } n = (r_a + r_b) \text{ mod } n = [(a \text{ mod } n) + (b \text{ mod } n)] \text{ mod } n$

Cont'd

- Examples of the three properties:

11 mod 8 = 3; 15 mod 8 = 7

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

(11 + 15) mod 8 = 26 mod 8 = 2

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

(11 - 15) mod 8 = - 4 mod 8 = 4

[(11 mod 8) * (15 mod 8)] mod 8 = 21 mod 8 = 5

(11 * 15) mod 8 = 165 mod 8 = 5

Practice: 11^7 mod 13

Arithmetic Modulo 8

- To find the additive inverse
  - Ex. (x + y) mod 8 = 0

+	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

(a) Addition modulo 8

Multiplication Modulo 8

- To find the multiplicative inverse
  - Ex. (x * y) mod 8 = 1 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

(b) Multiplication modulo 8

Additive and Multiplicative Inverses Modulo 8

- Not all integers mod 8 have a multiplicative inverse

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

(c) Additive and multiplicative inverses modulo 8

Properties of Modular Arithmetic

- The set of residues, or residue classes (mod *n*) Z_n: the set of nonnegative integers less than *n*
- $Z_n = \{0, 1, \ldots, (n-1)\}$, Z_n is a residual class
- The residue classes (mod *n*) as [0], [1],…[n-1], where $[r] = \{a: a \text{ is an integer}, a \equiv r \pmod{n}\}$

The residue classes (mod 4) are

$$[0] = \{\ldots, -16, -12, -8, -4, 0, 4, 8, 12, 16, \ldots\}$$
$$[1] = \{\ldots, -15, -11, -7, -3, 1, 5, 9, 13, 17, \ldots\}$$
$$[2] = \{\ldots, -14, -10, -6, -2, 2, 6, 10, 14, 18, \ldots\}$$
$$[3] = \{\ldots, -13, -9, -5, -1, 3, 7, 11, 15, 19, \ldots\}$$

n=4,
the residual class $Z_n = Z_4 = \{0, 1, 2, 3\}$

- Finding the smallest nonnegative integer to which k is congruent modulo *n* is called reducing k modulo n

Properties of Modular Arithmetic for Integers in Z_n

- If we perform modular arithmetic within Z_n, the properties shown in this table hold for integers in Z_n

Property	Expression
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 Law	$[w \times (x + y)] \bmod n = [(w \times x) + (w \times y)] \bmod n$
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 $w + z \equiv 0 \bmod n$

Cont'd

- Additive case:
  - If $(a+b) \equiv (a+c)(mod\ n)$ then $b \equiv c(mod\ n)$
    - Ex. (5+23) ≡ (5+7)(mod 8); 23 ≡7(mod 8)
  - Then adding the additive inverse of *a:*
    $((-a)+a+b) \equiv ((-a)+a+c)(mod\ n)$ then $b \equiv c(mod\ n)$
- Multiplicative case
  - If $(a*b) \equiv (a*c)(mod\ n)$ then $b \equiv c(mod\ n)$ if a is relatively prime to *n*
  - Then applying the multiplicative inverse of *a*:
    $((a\text{-}1)ab) \equiv ((a\text{-}1)ac)(mod\ n)$ *then* $b \equiv c(mod\ n)$

Ex.
6*3 = 18 ≡ $2(mod\ 8)$
6*7 = 42 ≡ $2(mod\ 8)$
Yet 3 /≡ 7(mod 8) because 6 and 8 are not relatively prime

Extended Euclidean Algorithm Example

- Euclidean algorithm:
  For any integers *a*, *b*, with *a≥b≥0*
  $$\gcd(a, b) = \gcd(b, a \bmod b)$$
  $$\gcd(55, 22) = \gcd(22, 55 \bmod 22) = \gcd(22, 11) = 11$$
- This can be used to determine the gcd:
  $$\gcd(18, 12) = \gcd(12, 6) = \gcd(6, 0) = 6$$
  $$\gcd(11, 10) = \gcd(10, 1) = \gcd(1, 0) = 1$$
- The extended Euclidean algorithm:
  $$ax + by = d = \gcd(a, b)$$

Extended cont'd

- Ex. a = 42, b = 30
  gcd(42, 30) = 6 then 42x+30y = 6(7x+5y)
- The smallest positive *value* of *ax*+*by* = *gcd(a, b)*

Extended Euclidean Algorithm			
Calculate	**Which satisfies**	**Calculate**	**Which satisfies**
$r_{-1} = a$		$x_{-1} = 1; y_{-1} = 0$	$a = ax_{-1} + by_{-1}$
$r_0 = b$		$x_0 = 0; y_0 = 1$	$b = ax_0 + by_0$
$r_1 = a \bmod b$ $q_1 = \lfloor a/b \rfloor$	$a = q_1 b + r_1$	$x_1 = x_{-1} - q_1 x_0 = 1$ $y_1 = y_{-1} - q_1 y_0 = -q_1$	$r_1 = ax_1 + by_1$
$r_2 = b \bmod r_1$ $q_2 = \lfloor b/r_1 \rfloor$	$b = q_2 r_1 + r_2$	$x_2 = x_0 - q_2 x_1$ $y_2 = y_0 - q_2 y_1$	$r_2 = ax_2 + by_2$
$r_3 = r_1 \bmod r_2$ $q_3 = \lfloor r_1/r_2 \rfloor$	$r_1 = q_3 r_2 + r_3$	$x_3 = x_1 - q_3 x_2$ $y_3 = y_1 - q_3 y_2$	$r_3 = ax_3 + by_3$
• • •	• • •	• • •	• • •
$r_n = r_{n-2} \bmod r_{n-1}$ $q_n = \lfloor r_{n-2}/r_{n-3} \rfloor$	$r_{n-2} = q_n r_{n-1} + r_n$	$x_n = x_{n-2} - q_n x_{n-1}$ $y_n = y_{n-2} - q_n y_{n-1}$	$r_n = ax_n + by_n$
$r_{n+1} = r_{n-1} \bmod r_n = 0$ $q_{n+1} = \lfloor r_{n-1}/r_{n-2} \rfloor$	$r_{n-1} = q_{n+1} r_n + 0$		$d = \gcd(a, b) = r_n$ $x = x_n; y = y_n$

Extended cont’d

- Ex. a = 1759, b = 550 and solve for 1759x+550y = gcd(1759, 550)

i	r_i	q_i	x_i	Y_i
–1	1759		1	0
0	550		0	1
1	109	3	1	–3
2	5	5	–5	16
3	4	21	106	–339
4	1	1	–111	355
5	0	4		

Result: $d = 1$; $x = -111$; $y = 355$

Groups

- A group G, denoted by {*G*, •} is a set of elements with a binary operation denoted by • that associates to each ordered pair (*a, b*) of elements in *G* an element (*a* • *b*) in *G* , such that the following axioms are obeyed:
- (A1) Closure:
  - If *a* and *b* belong to *G*, then *a* • *b* is also in *G*
- (A2) Associative:
  - *a* • *(b* • *c)* = *(a* • *b)* • *c* for all *a, b, c* in *G*
- (A3) Identity element:
  - There is an element *e* in *G* such that *a* • *e* = *e* • *a* = *a* for all *a* in *G*
- (A4) Inverse element:
  - For each *a* in *G*, there is an element *a'* in *G* such that *a*•*a'* = *a'* • *a* = *e*
- (A5) Commutative:
  - *a* • *b* = *b* • *a* for all *a, b* in *G*
  - A group is called **abelian** if it satisfies the condition above

- Finite group: a group has a finite number of elements <-> infinite group
- The order of the group = the number of elements in the group

Cyclic Group

- **Exponentiation** is defined within a group as a repeated application of the group operator, so that $a^3 = a \bullet a \bullet a$
- We define $a^0 = e$ as the **identity element**, and $a^{-n} = (a')^n$, where a' is the **inverse element** of a within the group

Ex. {2, 2^2, 2^3, etc.}

- A group G is **cyclic** if every element of G is a power a^k (k is an integer) of a fixed element
- The element a is said to **generate** the group G or to be a **generator** of G
- A cyclic group is always abelian and may be finite or infinite

Rings

- A ring R , sometimes denoted by $\{R , + , \times \}$, is a set of elements with two binary operations, called addition and multiplication, such that for all *a* , *b* , *c* in *R* the following axioms are obeyed:
  - (A1–A5)
    - R is an abelian group with respect to addition; that is, *R* satisfies axioms A1 through A5. For the case of an additive group, we denote the **identity element as 0** and the **inverse of *a* as –*a***
  - (M1) Closure under multiplication:
    - If *a* and *b* belong to *R* , then *ab* is also in *R*
  - (M2) Associativity of multiplication:
    - $a(bc) = (ab)c$ *for all* a , b , c *in* R
  - (M3) Distributive laws:
    - $a (b + c) = ab + ac$ *for all* a , b , c *in* R
    - $(a + b)c = ac + bc$ *for all* a , b , c *in* R

- In essence, a ring is a set in which we can do addition, subtraction [a - b = a + (-b)], and multiplication without leaving the set

Rings cont'd

- A ring is said to be commutative if it satisfies the following additional condition:
  - (M4) Commutativity of multiplication:
    - *ab = ba for all a, b in R*
- An integral domain is a commutative ring that obeys the following axioms.
  - (M5) Multiplicative identity:
    - There is an element 1 in *R* such that *a1 = 1a = a for all a in R*
  - (M6) No zero divisors:
    - *If a , b in R and ab = 0, then either a = 0 or b = 0*

Fields

- A field F, sometimes denoted by $\{F, +, \times\}$, is a set of elements with two binary operations, called addition and multiplication, such that for all *a, b, c* in *F* the following axioms are obeyed:
  - (A1–M6)
    - *F* is an integral domain; that is, *F* satisfies axioms A1 through A5 and M1 through M6
  - (M7) Multiplicative inverse:
    - For each *a* in *F*, except 0, there is an element a^{-1} in *F* such that $aa^{-1} = (a^{-1})a = 1$
- A field is a set in which we can do addition, subtraction, multiplication, and division without leaving the set. Division is defined with the following rule: $a/b = a(b^{-1})$

Familiar examples of fields are the rational numbers, the real numbers, and the complex numbers. Note that the set of all integers is not a field, because not every element of the set has a multiplicative inverse.

Group, Ring, and Field (6e)

FIELD

(A1) Closure under addition:	If a and b belong to S, then $a + b$ is also in S
(A2) Associativity of addition:	$a + (b + c) = (a + b) + c$ for all a, b, c in S
(A3) Additive identity:	There is an element 0 in R such that $a + 0 = 0 + a = a$ for all a in S
(A4) Additive inverse:	For each a in S there is an element $-a$ in S such that $a + (-a) = (-a) + a = 0$

Integral Domain

(A5) Commutativity of addition:	$a + b = b + a$ for all a, b in S

Commutative Ring

(M1) Closure under multiplication:	If a and b belong to S, then ab is also in S
(M2) Associativity of multiplication:	$a(bc) = (ab)c$ for all a, b, c in S
(M3) Distributive laws:	$a(b + c) = ab + ac$ for all a, b, c in S $(a + b)c = ac + bc$ for all a, b, c in S

Ring

(M4) Commutativity of multiplication:	$ab = ba$ for all a, b in S

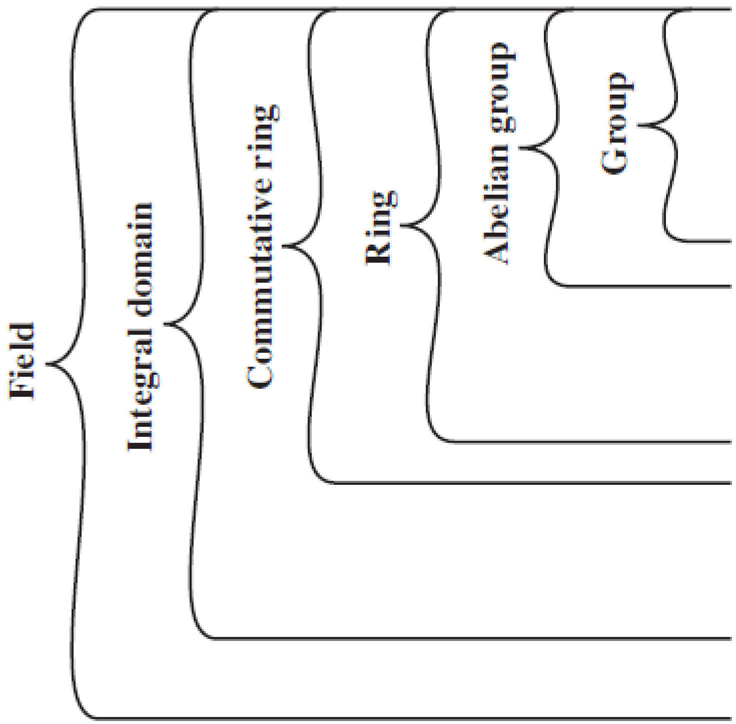
Abelian Group

(M5) Multiplicative identity:	There is an element 1 in S such that $a1 = 1a = a$ for all a in S
(M6) No zero divisors:	If a, b in S and $ab = 0$, then either $a = 0$ or $b = 0$

Group

(M7) Multiplicative inverse:	If a belongs to S and $a \neq 0$, there is an element a^{-1} in S such that $aa^{-1} = a^{-1}a = 1$

Group, Ring, and Field (5e)



(A1) Closure under addition:	If a and b belong to S, then $a + b$ is also in S
(A2) Associativity of addition:	$a + (b + c) = (a + b) + c$ for all a, b, c in S
(A3) Additive identity:	There is an element 0 in R such that $a + 0 = 0 + a = a$ for all a in S
(A4) Additive inverse:	For each a in S there is an element $-a$ in S such that $a + (-a) = (-a) + a = 0$
(A5) Commutativity of addition:	$a + b = b + a$ for all a, b in S
(M1) Closure under multiplication:	If a and b belong to S, then ab is also in S
(M2) Associativity of multiplication:	$a(bc) = (ab)c$ for all a, b, c in S
(M3) Distributive laws:	$a(b + c) = ab + ac$ for all a, b, c in S $(a + b)c = ac + bc$ for all a, b, c in S
(M4) Commutativity of multiplication:	$ab = ba$ for all a, b in S
(M5) Multiplicative identity:	There is an element 1 in S such that $a1 = 1a = a$ for all a in S
(M6) No zero divisors:	If a, b in S and $ab = 0$, then either $a = 0$ or $b = 0$
(M7) Multiplicative inverse:	If a belongs to S and a 0, there is an element a^{-1} in S such that $aa^{-1} = a^{-1}a = 1$

Figure 4.2 Groups, Ring, and Field

Finite Fields of the Form GF(*p*)

- Finite fields play a crucial role in many cryptographic algorithms
- GF(p^n): the finite field of order p^n, *GF: Galois field*
  - The order of a finite field (the number of elements in the field) must be a power of a prime p^n, where n is a positive integer
  - GF stands for Galois field, in honor of the mathematician who first studied finite fields
  - GF(p): the finite field of order p (for a prime p). The set Z_p of integers $\{0, 1, \ldots, p-1\}$

Cont’d

- P is prime
- GF(p^n):
  - The order of this finite field: p^n
- GF(p):
  - Special case when n=1
  - The order of this finite field: p
- GF(2^n)
  - Special case of non-prime base

Recall: Properties of Modular Arithmetic

- The residue classes (mod *p*) Z_p = {0, 1,…, (p-1)}
- The residue classes (mod *p*) as [0], [1],…[p-1], where [*r*] = {*a*: *a* is an integer, $a \equiv r \pmod p$}

The residue classes (mod 4) are

$$
\begin{aligned}
[0] &= \{\ldots, -16, -12, -8, -4, 0, 4, 8, 12, 16, \ldots\} \\
[1] &= \{\ldots, -15, -11, -7, -3, 1, 5, 9, 13, 17, \ldots\} \\
[2] &= \{\ldots, -14, -10, -6, -2, 2, 6, 10, 14, 18, \ldots\} \\
[3] &= \{\ldots, -13, -9, -5, -1, 3, 7, 11, 15, 19, \ldots\}
\end{aligned}
$$

- Z_p is a commutative ring

Property	Expression
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 Law	$[w \times (x + y)] \bmod n = [(w \times x) + (w \times y)] \bmod n$
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 $w + z \equiv 0 \bmod n$

Properties for Z_p

- Any integer in Z_p has a **multiplicative inverse** if and only if that integer is relatively prime to p.
- If p is **prime**, then all of the nonzero integers in Z_p are **relatively prime** to p, and therefore there exists a **multiplicative inverse** for all of the nonzero integers in Z_p.
- Thus, for Z_p we can add the following properties:

Multiplicative inverse (w^{-1})	For each $w \in Z_p$, $w \neq 0$, there exists a $z \in Z_p$ such that $w \times z \equiv 1 \pmod{p}$

Cont'd

Multiplicative inverse (w^{-1})	For each $w \in Z_p$, $w \neq 0$, there exists a $z \in Z_p$ such that $w \times z \equiv 1 \pmod{p}$

- Because *w* is relatively prime to *p*, if we multiply all the elements of Z_p by w, the resulting residues are all of the elements of Z_p permuted.
- Thus, exactly one of the residues has the value 1.
- Therefore, there is some integer in Z_p that, when multiplied by *w*, yields the residue 1.
- The integer is the multiplizative inverse of *w*, designated w^{-1}.
- Therefore, Z_p is in fact a finite field.

Arithmetic in GF(7)

- Example: p=7=prime, GF(p)=GF(7)
- Can we find?
  - Additive Inverse
  - Multiplication Inverse
    - According to previous properties,

Multiplicative inverse (w^{-1})	For each $w \in Z_p$, $w \neq 0$, there exists a $z \in Z_p$ such that $w \times z \equiv 1 \pmod{p}$

We can find w^{-1}

Cont’d

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

(a) Addition modulo 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

(b) Multiplication modulo 7

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

(c) Additive and multiplicative inverses modulo 7

Example of GF(2)

The simplest finite field is GF(2). Its arithmetic operations are easily summarized:

$+$	0	1
0	0	1
1	1	0

Addition

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

Multiplication

w	$-w$	w^{-1}
0	0	—
1	1	1

Inverses

In this case, addition is equivalent to the exclusive-OR (XOR) operation, and multiplication is equivalent to the logical AND operation.

Finding the Multiplicative Inverse in GF(*p*)

- It is easy to find the multiplicative inverse of an element in GF(p) for small values of p. For large value of p, this approach is not practical.
- If *a* and *b* are relatively prime, then *b* has a multiplicative inverse modulo *a*.
  - That is, if $gcd(a, b)=1$, then *b* has a multiplicative inverse modulo *a*.
  - That is, for positive integer $b < a$, there exists a $b^{-1} < a$ such that $bb^{-1} = 1 \bmod a$. If *a* is a prime number and $b < a$, then clearly *a* and *b* are relatively prime and have a gcd divisor of 1.
  - Ex. gcd(7, 3)=1, we can find a $b^{-1} < a$ such that $bb^{-1} = 1 \bmod a$. *We can find* $b^{-1} = 5$ *satisfies* $(3)(5) = 1 \bmod 7$
- Now we can easily compute b^{-1} using the extended Euclidean algorithm.

Finding cont'd

- Extended Euclidean algorithm

$$ax + by = d = \gcd(a, b)$$

If $gcd(a, b) = 1$ then we have $ax + by = 1$

$$[(ax \bmod a) + (by \bmod a)] \bmod a = 1 \bmod a$$

$$\boxed{0 + (by \bmod a) = 1}$$

But if $\underline{by \bmod a = 1}$, then $\underline{y = b^{-1}}$

Thus, applying the extended Euclidean algorithm we can yield the value of the multiplicative inverse of b if $gcd(a, b)=1$.

- Extended Euclidean can:

1. Find gcd(a,b)
2. Find multiplicative inverse of b if gcd(a,b)=1

Example

- a=1759 (prime number), b=550
  - ax+by = d = gcd(a, b)
  - *1759x + 550y = d = gcd(1759, 550)*
  - Results: d = 1; x = -111; y=*355*.
    Thus, b^{-1} = *355*.
    verify, we calculate *550*355 mod 1759 = 195250 mod 1759 = 1*. (*by mod a = 1*)

The extended Euclidean algorithm can be used to find a multiplicative inverse in Z_n for any n. If we apply the extended Euclidean algorithm to the equation $nx + by = d$, and the algorithm yields $d = 1$, then $y=b^{-1}$ in Z_n.

Short Summary

- In this section, we have shown how to construct a finite field of order *p*, where *p* is prime.
- GF(*p*) is defined with the following properties:
  - GF(*p*) consists of *p* elements
  - The binary operations + and x are defined over the set. The operations of addition, subtraction, multiplication, and division can be performed without leaving the set. Each element of the set other than 0 has a multiplicative inverse
  - We have shown that the elements of GF(*p*) are the integers {0, 1, . . . , *p* – 1} and that the arithmetic operations are addition and multiplication mod *p*

Polynomial Arithmetic

- We can distinguish three classes of polynomial arithmetic:

- 1. Ordinary polynomial arithmetic, using the basic rules of algebra

- 2. Polynomial arithmetic in which the arithmetic on the coefficients is performed modulo *p*; that is, the coefficients are in GF(*p*)

- 3. Polynomial arithmetic in which the coefficients are in GF(*p*), and the polynomials are defined modulo a polynomial *m (x)* whose highest power is some integer *n*

1. Ordinary Polynomial

- A polynomial of degree *n* (integer *n≥0*) is an expression of the form

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

  - where that a_i are elements of some designated set of number *S*, called the coefficient set, and $a_n \neq 0$.
  - We say that such polynomials are defined over the coefficient set *S*

- Polynomial arithmetic includes the operations of *addition*, *subtraction*, and *multiplication*

- Division is similarly defined, but requires that *S* be a field.
  - Ex.real numbers, rational numbers, and Z_p for *p* prime.

Ordinary cont'd

- In the form:

$$f(x) = \sum_{i=0}^{n} a_i x^i; \qquad g(x) = \sum_{i=0}^{m} b_i x^i; \qquad n \geq m$$

- Addition

$$f(x) + g(x) = \sum_{i=0}^{m} (a_i + b_i)x^i + \sum_{i=m+1}^{n} a_i x^i$$

- Multiplication

$$f(x) \times g(x) = \sum_{i=0}^{n+m} c_i x^i$$

$$c_k = a_0 b_k + a_1 b_{k-1} + \cdots + a_{k-1} b_1 + a_k b_0$$

Ordinary Polynomial Arithmetic Example

- Example:

  let $f(x) = x^3 + x^2 + 2$ and $g(x) = x^2 - x + 1$,
  where S is the set of integers

$f(x) + g(x) = x^3 + 2x^2 - x + 3$

$$\begin{array}{rrrr}
 & x^3 + x^2 & & + \ 2 \\
+ & (x^2 - x & + & 1) \\
\hline
 & x^3 + 2x^2 - x & + & 3
\end{array}$$

(a) Addition

$f(x) - g(x) = x^3 + x + 1$

$$\begin{array}{rrrr}
 & x^3 + x^2 & & + \ 2 \\
- & (x^2 - x & + & 1) \\
\hline
 & x^3 \quad + x & + & 1
\end{array}$$

(b) Subtraction

$f(x) * g(x) = x^5 + 3x^2 - 2x + 2$

$$\begin{array}{r}
x^3 + x^2 \qquad + 2 \\
\times \ (x^2 - x + 1) \\
\hline
x^3 + x^2 \qquad + 2 \\
- x^4 - x^3 \qquad - 2x \quad \\
x^5 + x^4 \qquad + 2x^2 \qquad \\
\hline
x^5 \qquad + 3x^2 - 2x + 2
\end{array}$$

(c) Multiplication

$$\begin{array}{r}
x + 2 \\
x^2 - x + 1 \,\big)\, \overline{x^3 + x^2 \qquad + 2} \\
x^3 - x^2 + x \qquad \\
\hline
2x^2 - x + 2 \\
2x^2 - 2x + 2 \\
\hline
x \quad
\end{array}$$

(d) Division

2. Polynomial Arithmetic With Coefficients in Z_p

- Now consider polynomials in which the coefficients are elements of some field F;
  - refer to this as a polynomial over the field F.
- It is easy to show that the set of such polynomials is a ring, referred to as a polynomial ring.
  - That is, if we consider each distinct polynomial to be an element of the set, then that set is a ring.

Ex. $f(x)=ax^2+bx+c$, $g(x)=dx+e$
Field F = {a, b, c, d, e}
Ring R = {f(x), g(x)}

Polynomial ring cont'd

- When polynomial arithmetic is performed on polynomials over a field, then division is possible
  - Note: this does not mean that *exact division* is possible
  - i.e. within a field, given two elements *a* and *b*, the quotient *a/b* is also an element of the field
- However, given a ring *R* that is not a field, division will result in both a quotient and a remainder; this is not exact division

Example

- The division 5/3 within a set *S*
  - If *S* is the set of rational numbers(field)
    - the result is imply expressed as 5/3 and is an element of S
  - If S is the field Z_7(field)
    - $5/3 = (5*3^{-1}) \bmod 7 = (5*5) \bmod 7 = 4$ (table 4.5c)
    - Polynomial example: $(5x^2)/(3x) = 4x$, valid polynomial coefficient in Z_7
  - If S is the set of integers (a ring but not a field)
    - 5/3 produces a quotient of 1 and a remainder of 2
      $5/3 = 1+2/3$
      Polynomial example: coefficient 5/3 is not in the set
    - division is not exact over the set of integers

If we attempt to perform polynomial division over a coefficient set that is not a field, we find that division is not always defined->not meaningful

Polynomial Division

- But –
  Even if the coefficient set is a field, polynomial division is not necessarily exact (but polynomial division is possible if the coefficient set is a field)
- Given polynomials $f(x)$ and $g(x)$, if we divide $f(x)$ by $g(x)$, we get a quotient $q(x)$ and a remainder $r(x)$
  - $f(x)/g(x) = q(x) + r(x)/g(x)$ *or* $f(x) = q(x)g(x) + r(x)$
  - *The polynomial degrees are*
    - *Degree* $f(x) = n$
    - *Degree* $g(x) = m$
    - *Degree* $q(x) = n-m$
    - *Degree* $r(x) \leq m-1$

- The remainders are allowed, therefore, polynomial division is possible if the coefficient set is a field

Polynomial Division cont'd

- Polynomial in the form: $f(x) = q(x)\, g(x) + r(x)$
  - Remainder can be represented as:
    $r(x) = f(x) \bmod g(x)$
  - If there is no remainder we can say $g(x)$ divides $f(x)$
    - Written as $g(x) \mid f(x)$
    - i.e. $g(x)$ is a factor of $f(x)$ or $g(x)$ is a divisor of $f(x)$

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

(d) Division

Polynomials over GF(2)

- Polynomial arithmetic over GF(2)
  - Example:
    $f(x) = x^7+x^5+x^4+x^3+x+1$, $g(x) = x^3 + x + 1$
  - Recall: Addition is equivalent to XOR and Multiplication is equal to AND

+	0	1
0	0	1
1	1	0

Addition

×	0	1
0	0	0
1	0	1

Multiplication

$$
\begin{array}{r}
x^7 + x^5 + x^4 + x^3 + x + 1 \\
+ (x^3 + x + 1) \\
\hline
x^7 + x^5 + x^4 \qquad\qquad\qquad
\end{array}
$$

(a) Addition

$$
\begin{array}{r}
x^7 + x^5 + x^4 + x^3 + x + 1 \\
- (x^3 + x + 1) \\
\hline
x^7 + x^5 + x^4 \qquad\qquad\qquad
\end{array}
$$

(b) Subtraction

Cont’d

$$
\begin{array}{r}
x^7 + x^5 + x^4 + x^3 + x + 1 \\
\times\ (x^3 + x + 1) \\
\hline
x^7 + x^5 + x^4 + x^3 + x + 1 \\
x^8 + x^6 + x^5 + x^4 + x^2 + x \\
x^{10} + x^8 + x^7 + x^6 + x^4 + x^3 \\
\hline
x^{10} + x^4 + x^2 + 1
\end{array}
$$

(c) Multiplication

- Recall: There is no remainder, so g(x) divides f(x)
  - Written as g(x) | f(x)
  - i.e. g(x) is a factor of f(x) or g(x) is a divisor of f(x)

$$
\begin{array}{r l}
 & x^4 + 1 \\
\cline{2-2}
x^3 + x + 1 \,\big) & x^7 + x^5 + x^4 + x^3 + x + 1 \\
 & x^7 + x^5 + x^4 \\
\cline{2-2}
 & x^3 + x + 1 \\
 & x^3 + x + 1 \\
\cline{2-2}
\end{array}
$$

(d) Division

Polynomial Division

- A polynomial f(x) over a field F is called irreducible polynomial (also called a prime polynomial)
  - if and only 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)
  - Ex. $f(x) = x^4+1$ over GF(2) is reducible, because

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

Finding Polynomial GCD

- The polynomial *c(x)* is said to be the greatest common divisor of *a(x)* and *b(x)* if the following are true:
  - *c(x)* divides both *a(x)* and *b(x)*
  - Any divisor of *a(x)* and *b(x)* is a divisor of *c(x)*
- An equivalent definition is:
  - *gcd[a(x), b(x)]* is the polynomial of maximum degree that divides both *a(x)* and *b(x)*

Cont'd

- The Euclidean algorithm can be extended to find the greatest common divisor of two polynomials whose coefficients are elements of a field

$$\boxed{\gcd[a(x), b(x)] = \gcd[b(x), a(x) \bmod b(x)]}$$

Assume the degree of a(x) is greater than the degree of b(x)

Euclidean Algorithm for Polynomials	
Calculate	**Which satisfies**
$r_1(x) = a(x) \bmod b(x)$	$a(x) = q_1(x)b(x) + r_1(x)$
$r_2(x) = b(x) \bmod r_1(x)$	$b(x) = q_2(x)r_1(x) + r_2(x)$
$r_3(x) = r_1(x) \bmod r_2(x)$	$r_1(x) = q_3(x)r_2(x) + r_3(x)$
• • •	• • •
$r_n(x) = r_{n-2}(x) \bmod r_{n-1}(x)$	$r_{n-2}(x) = q_n(x)r_{n-1}(x) + r_n(x)$
$r_{n+1}(x) = r_{n-1}(x) \bmod r_n(x) = 0$	$r_{n-1}(x) = q_{n+1}(x)r_n(x) + 0$ $d(x) = \gcd(a(x), b(x)) = r_n(x)$

At each iteration, we have $d(x) = \gcd(r_{i+1}(x), r_i(x))$ until finally $d(x) = \gcd(r_n(x), 0) = r_n(x)$

Find $\gcd[a(x), b(x)]$ for $a(x) = x^6 + x^5 + x^4 + x^3 + x^2 + x + 1$ and $b(x) = x^4 + x^2 + x + 1$. First, we divide $a(x)$ by $b(x)$:

$$
\begin{array}{r@{\,}l}
 & x^2 + x \\ \cline{2-2}
x^4 + x^2 + x + 1 \,\big) & x^6 + x^5 + x^4 + x^3 + x^2 + x + 1 \\
 & x^6 \phantom{{}+x^5} + x^4 + x^3 + x^2 \\ \cline{2-2}
 & \phantom{x^6 +{}} x^5 \phantom{{}+x^4+x^3+x^2} + x + 1 \\
 & \phantom{x^6 +{}} x^5 \phantom{{}+x^4} + x^3 + x^2 + x \\ \cline{2-2}
 & \phantom{x^6 + x^5 + x^4 +{}} x^3 + x^2 \phantom{{}+x} + 1
\end{array}
$$

This yields $r_1(x) = x^3 + x^2 + 1$ and $q_1(x) = x^2 + x$.
Then, we divide $b(x)$ by $r_1(x)$.

$$
\begin{array}{r@{\,}l}
 & x + 1 \\ \cline{2-2}
x^3 + x^2 + 1 \,\big) & x^4 \phantom{{}+x^3} + x^2 + x + 1 \\
 & x^4 + x^3 \phantom{{}+x^2} + x \\ \cline{2-2}
 & \phantom{x^4 +{}} x^3 + x^2 \phantom{{}+x} + 1 \\
 & \phantom{x^4 +{}} x^3 + x^2 \phantom{{}+x} + 1 \\ \cline{2-2}
\end{array}
$$

This yields $r_2(x) = 0$ and $q_2(x) = x + 1$.
Therefore, $\gcd[a(x), b(x)] = r_1(x) = x^3 + x^2 + 1$.

Finite Fields of the Form $GF(2^n)$

- The order of a finite field must be of the form p^n, where p is a prime and n is a positive integer
- GF(p) (in the earlier slides): special case of finite fields with order p
  - Using modular arithmetic in Z_p, all of the axioms for a field are satisfied
  - but for polynomials over p^n, operations modulo p^n do not produce a field
  - focus on what structure satisfies the axioms for a field in a set with p^n elements

Virtually all encryption algorithm (symmetric and public key) involve arithmetic operations on integer. So we need to work in arithmetic defined over a field for division operation.

Cont’d

- Suppose we wish to use 3-bit blocks in the encryption algorithm, and use only the operations of addition and multiplication
  - Ex. Table 4.6 and Table 4.2
    - The number of occurrences of the nonzero integers is uniform for multiplication

Integer	1	2	3	4	5	6	7	
Occurrences in Z_8	4	8	4	12	4	8	4	Table 4.2
Occurrences in $GF(2^3)$	7	7	7	7	7	7	7	Table 4.6

    - Observations:
      - Even we are similarly interested 2^3 (= 8) modulo arithmetic but for $GF(2^3)$ that:
      - The Add./Mult. tables are symmetric about the main diagonal
      - All nonzero elements have a multiplicative inverse
      - The scheme satisfies all the requirements for a finite field

Table 4.2 Arithmetic Modulo 8

+	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

(a) Addition modulo 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

(b) Multiplication modulo 8

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

(c) Additive and multiplicative inverse modulo 8

Table 4.6 Arithmetic in $GF(2^3)$

	+	000 0	001 1	010 2	011 3	100 4	101 5	110 6	111 7
000	0	0	1	2	3	4	5	6	7
001	1	1	0	3	2	5	4	7	6
010	2	2	3	0	1	6	7	4	5
011	3	3	2	1	0	7	6	5	4
100	4	4	5	6	7	0	1	2	3
101	5	5	4	7	6	1	0	3	2
110	6	6	7	4	5	2	3	0	1
111	7	7	6	5	4	3	2	1	0

(a) Addition

	×	000 0	001 1	010 2	011 3	100 4	101 5	110 6	111 7
000	0	0	0	0	0	0	0	0	0
001	1	0	1	2	3	4	5	6	7
010	2	0	2	4	6	3	1	7	5
011	3	0	3	6	5	7	4	1	2
100	4	0	4	3	7	6	2	5	1
101	5	0	5	1	4	2	7	3	6
110	6	0	6	7	1	5	3	2	4
111	7	0	7	5	2	1	6	4	3

(b) Multiplication

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

(c) Additive and multiplicative inverses

Modular Polynomial Arithmetic

- Consider the set S of all polynomials of degree $n-1$ or less over the field Z_p. Thus, each polynomial has the form

$$f(x) = a_{n-1}x^{n-1} + a_{n-2}x^{n-2} + \cdots + a_1x + a_0 = \sum_{i=0}^{n-1} a_ix^i$$

where each a_i takes on a value in the set {0,1,…,p-1}

- There are a total of p^n different polynomials in S

For $p = 3$ and $n = 2$, the $3^2 = 9$ polynomials in the set are

0	x	$2x$
1	$x + 1$	$2x + 1$
2	$x + 2$	$2x + 2$

For $p = 2$ and $n = 3$, the $2^3 = 8$ polynomials in the set are

0	$x + 1$	$x^2 + x$
1	x^2	$x^2 + x + 1$
x	$x^2 + 1$	

Coefficient ai: {0, 1,…, p-1}
Degree: {n-1, …, 0}

Make *S* a Finite Field

- With the appropriate definition of arithmetic operations, each such set *S* is a finite field:
  - 1.Arithmetic follows the ordinary rules of polynomial arithmetic using the basic rules of algebra, with the following two refinements.
  - 2. Arithmetic on the coefficients is performed modulo p. That is, we use the rules of arithmetic for the finite field Zp.
  - 3. If multiplication results in a polynomial of degree greater than n - 1, then the polynomial is reduced modulo some irreducible polynomial m(x) of degree n. That is, we divide by m(x) and keep the remainder. For a polynomial f(x), the remainder is expressed as r(x) = f(x) mod m(x).

Cont'd

- Example: Advanced Encryption Standard (AES) uses arithmetic in the finite field GF(2^8), with the irreducible polynomial $m(x) = x^8+x^4+x^3+x+1$. Consider the two polynomials $f(x) = x^6+x^4+x^2+x+1$ and $g(x) = x^7+x+1$, the result of $f(x)*g(x) \ mod \ m(x)$ is:

$$
\begin{aligned}
f(x) \times g(x) &= x^{13} + x^{11} + x^9 + x^8 + x^7 \\
&\quad + x^7 + x^5 + x^3 + x^2 + x \\
&\quad + x^6 + x^4 + x^2 + x + 1 \\
&= x^{13} + x^{11} + x^9 + x^8 + x^6 + x^5 + x^4 + x^3 + 1
\end{aligned}
$$

$$
\begin{array}{r|l}
 & x^5 + x^3 \\
\hline
x^8 + x^4 + x^3 + x + 1 & x^{13} + x^{11} + x^9 + x^8 + x^6 + x^5 + x^4 + x^3 + 1 \\
 & x^{13} + x^9 + x^8 + x^6 + x^5 \\
\cline{2-2}
 & x^{11} + x^4 + x^3 \\
 & x^{11} + x^7 + x^6 + x^4 + x^3 \\
\cline{2-2}
 & x^7 + x^6 + 1
\end{array}
$$

$$f(x) \times g(x) \bmod m(x) = x^7 + x^6 + 1$$

The set of residues modulo $m(x)$, an nth-degree polynomial, consists of p^n elements. Each of these elements is represented by one of the p^n polynomials of degree $m < n$.

Cont'd

- Other properties of modular polynomial arithmetic:
  - The set of residues modulo *m(x)*, an *n*th-degree polynomial, consists of p^n elements.
  - Each of these elements is represented by one of the p^n polynomials of degree $m<n$.
- Congruent

> The residue class $[x + 1]$, $(\bmod\, m(x))$, consists of all polynomials $a(x)$ such that $a(x) \equiv (x + 1) \pmod{m(x)}$. Equivalently, the residue class $[x + 1]$ consists of all polynomials $a(x)$ that satisfy the equality $a(x) \bmod m(x) = x + 1$.

To Construct the Finite Field GF(2^3)

- To construct the finite field GF(2^3), we need to choose an irreducible polynomial of degree 3. There are only two such polynomials: $(x^3 + x^2 + 1)$ and $(x^3 + x + 1)$.
  - Table 4.7 use the 2nd to show the addition and multiplication tables for GF(2^3).
    Table 4.7 has the identical structure to those of Table 4.6.

Cont’d

Table 4.7 Polynomial Arithmetic Modulo $(x^3 + x + 1)$

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

Ex. consider binary 100 + 010 = 110. This is equivalent to $x^2 + x$

Cont’d

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

(b) Multiplication

Also consider 100 * 010 = 011, which is equivalent to x^2 * x = x3 and reduces to x + 1. That is, x^3 mod (x^3 + x + 1) = x + 1, which is equivalent to 011.

Finding the Multiplicative Inverse

- Just like the Euclidean algorithm can be adapted to find the gcd of two polynomials, the extended Euclidean algorithm can be adapted to find the multiplicative inverse of a polynomial.
- Given polynomials *a(x)* and *b(x)* with the degree of *a(x)* greater than the degree of *b(x)*, we wish to solve the following equation for the values *v(x), w(x),* and *d(x)*, where *d(x)=gcd[a(x), b(x)]*:

$$a(x)v(x) + b(x)w(x) = d(x)$$

  – If *d(x)=1*, then is the multiplicative inverse of *b(x)* modulo *a(x)*.

Recall

- Extended Euclidean algorithm

$$ax + by = d = \gcd(a, b)$$

If *gcd(a, b) = 1* then we have *ax + by = 1*

$$[(ax \bmod a) + (by \bmod a)] \bmod a = 1 \bmod a$$

$$\boxed{0 + (by \bmod a) = 1}$$

But if *by mod a =1*, then $y=b^{-1}$

Thus, applying the extended Euclidean algorithm we can yield the value of the multiplicative inverse of *b* if *gcd(a, b)=1*.

- Extended Euclidean can:

1. Find gcd(a,b)
2. Find multiplicative inverse of b if gcd(a,b)=1

Extended Euclidean Algorithm for Polynomials			
Calculate	**Which satisfies**	**Calculate**	**Which satisfies**
$r_{-1}(x) = a(x)$		$v_{-1}(x) = 1; w_{-1}(x) = 0$	$a(x) = a(x)v_{-1}(x) + bw_{-1}(x)$
$r_0(x) = b(x)$		$v_0(x) = 0; w_0(x) = 1$	$b(x) = a(x)v_0(x) + b(x)w_0(x)$
$r_1(x) = a(x) \bmod b(x)$ $q_1(x) =$ quotient of $a(x)/b(x)$	$a(x) = q_1(x)b(x) + r_1(x)$	$v_1(x) = v_{-1}(x) - q_1(x)v_0(x) = 1$ $w_1(x) = w_{-1}(x) - q_1(x)w_0(x) = -q_1(x)$	$r_1(x) = a(x)v_1(x) + b(x)w_1(x)$
$r_2(x) = b(x) \bmod r_1(x)$ $q_2(x) =$ quotient of $b(x)/r_1(x)$	$b(x) = q_2(x)r_1(x) + r_2(x)$	$v_2(x) = v_0(x) - q_2(x)v_1(x)$ $w_2(x) = w_0(x) - q_2(x)w_1(x)$	$r_2(x) = a(x)v_2(x) + b(x)w_2(x)$
$r_3(x) = r_1(x) \bmod r_2(x)$ $q_3(x) =$ quotient of $r_1(x)/r_2(x)$	$r_1(x) = q_3(x)r_2(x) + r_3(x)$	$v_3(x) = v_1(x) - q_3(x)v_2(x)$ $w_3(x) = w_1(x) - q_3(x)w_2(x)$	$r_3(x) = a(x)v_3(x) + b(x)w_3(x)$
• • •	• • •	• • •	• • •
$r_n(x) = r_{n-2}(x) \bmod r_{n-1}(x)$ $q_n(x) =$ quotient of $r_{n-2}(x)/r_{n-3}(x)$	$r_{n-2}(x) = q_n(x)r_{n-1}(x) + r_n(x)$	$v_n(x) = v_{n-2}(x) - q_n(x)v_{n-1}(x)$ $w_n(x) = w_{n-2}(x) - q_n(x)w_{n-1}(x)$	$r_n(x) = a(x)v_n(x) + b(x)w_n(x)$
$r_{n+1}(x) = r_{n-1}(x) \bmod r_n(x) = 0$ $q_{n+1}(x) =$ quotient of $r_{n-1}(x)/r_{n-2}(x)$	$r_{n-1}(x) = q_{n+1}(x)r_n(x) + 0$		$d(x) = \gcd(a(x), b(x)) = r_n(x)$ $v(x) = v_n(x); w(x) = w_n(x)$

Example

Table 4.8 Extended Euclid $[(x^8 + x^4 + x^3 + x + 1), (x^7 + x + 1)]$

Initialization	$a(x) = x^8 + x^4 + x^3 + x + 1; v_{-1}(x) = 1; w_{-1}(x) = 0$ $b(x) = x^7 + x + 1; v_0(x) = 0; w_0(x) = 1$
Iteration 1	$q_1(x) = x;\ r_1(x) = x^4 + x^3 + x^2 + 1$ $v_1(x) = 1; w_1(x) = x$
Iteration 2	$q_2(x) = x^3 + x^2 + 1;\ r_2(x) = x$ $v_2(x) = x^3 + x^2 + 1;\ w_2(x) = x^4 + x^3 + x + 1$
Iteration 3	$q_3(x) = x^3 + x^2 + x;\ r_3(x) = 1$ $v_3(x) = x^6 + x^2 + x + 1;\ w_3(x) = x^7$
Iteration 4	$q_4(x) = \mathrm{x};\ r_4(x) = 0$ $v_4(x) = x^7 + x + 1;\ w_4(x) = x^8 + x^4 + x^3 + x + 1$
Result	$d(x) = r_3(x) = \gcd(a(x), b(x)) = 1$ $w(x) = w_3(x) = (x^7 + x + 1)^{-1} \bmod (x^8 + x^4 + x^3 + x + 1) = x^7$

Therefore, the multiplicative is x^7 and

$$\boxed{(x^7 + x + 1)(x^7) \equiv 1(\bmod (x^8 + x^4 + x^3 + x + 1))}$$

Addition

- Polynomials in *GF(2ⁿ)*
  - Since coefficients are 0 or 1, they can represent any such polynomial as a bit string
- Addition becomes XOR of these bit strings
- Example

Consider the two polynomials in GF(2^8) from our earlier example:

$$f(x) = x^6 + x^4 + x^2 + x + 1 \text{ and } g(x) = x^7 + x + 1.$$

$(x^6 + x^4 + x^2 + x + 1) + (x^7 + x + 1)$	$=$	$x^7 + x^6 + x^4 + x^2$	(polynomial notation)
$(01010111) \oplus (10000011)$	$=$	(11010100)	(binary notation)
$\{57\} \oplus \{83\}$	$=$	$\{D4\}$	(hexadecimal notation)[10]

Multiplication

- Multiplication is shift and XOR
  - No simple XOR function (has to add intermediate results)
  - Example: 1.Modulo Reduction
    - $GF(2^8)$ use $m(x) = x^8 + x^4 + x^3 + x + 1$, and $x^8 \bmod m(x) = [m(x) - x^8] = (x^4 + x^3 + x + 1)$
    - In general, in $GF(2^n)$ with an nth-degree polynomial $p(x)$,we have $x^n \bmod p(x) = [p(x) - x^n]$
    - Now, consider a polynomial in $GF(2^8)$ that $f(x) = b_7x^7 + b_6x^6 + b_5x^5 + b_4x^4 + b_3x^3 + b_2x^2 + b_1x + b_0$. If we multiply by x, we have

$$x \times f(x) = (b_7x^8 + b_6x^7 + b_5x^6 + b_4x^5 + b_3x^4 + b_2x^3 + b_1x^2 + b_0x) \bmod m(x)$$

Cont'd

- If $b_7 = 0$, then the result is a polynomial of degree less than 8, which is already in reduced form, and no further computation is necessary.
- If $b_7 = 1$, then reduction modulo m(x) is achieved using Equation (4.12):
  - $x * f(x) = (b_6x^7 + b_5x^6 + b_4x^5 + b_3x^4 + b_2x^3 + b_1x^2 + b_0x) + (x^4 + x^3 + x + 1)$

i.e. $x^n * f(x) \bmod m(x)$

Now, consider a polynomial in GF(2^8),
the form $f(x) = b_7x^7 + b_6x^6 + b_5x^5 + b_4x^4 + b_3x^3 + b_2x^2 + b_1x + b_0$

If we multiply by x

$$x \times f(x) = (b_7x^8 + b_6x^7 + b_5x^6 + b_4x^5 + b_3x^4 + b_2x^3 + b_1x^2 + b_0x) \bmod m(x)$$

If $b_7 = 0$

$$x \times f(x) = b_6x^7 + b_5x^6 + b_4x^5 + b_3x^4 + b_2x^3 + b_1x^2 + b_0x$$

If $b_7 = 1$

$$x \times f(x) = (\boxed{b_7x^8} + b_6x^7 + b_5x^6 + b_4x^5 + b_3x^4 + b_2x^3 + b_1x^2 + b_0x) \boxed{\bmod m(x)}$$
$$= (b_6x^7 + b_5x^6 + b_4x^5 + b_3x^4 + b_2x^3 + b_1x^2 + b_0x) + \boxed{(x^4 + x^3 + x + 1)}$$

Recall: GF(2^8) use $m(x) = x^8 + x^4 + x^3 + x + 1$, and x^8 mod $m(x) = [m(x) - x^8] = (x^4 + x^3 + x + 1)$

Binary Notation

- 2.conditional bitwise XOR with (000011011)
- Multiplication by *x* (i.e., 00000010) can be implemented as a 1-bit left shift followed by a conditional bitwise XOR with (00011011), which represents (x^4+x^3+x+1)
- $$x \times f(x) = \begin{cases} (b_6b_5b_4b_3b_2b_1b_0 0) & \text{if } b_7 = 0 \\ (b_6b_5b_4b_3b_2b_1b_0 0) \oplus (00011011) & \text{if } b_7 = 1 \end{cases}$$

Multiplication by a higher power of *x* can be achieved by repeated application of the equation above. By adding intermediate results, multiplication by any constant in $GF(2^8)$ can be achieved

Example

In an earlier example, we showed that for $f(x) = x^6 + x^4 + x^2 + x + 1$, $g(x) = x^7 + x + 1$, and $m(x) = x^8 + x^4 + x^3 + x + 1$, we have $f(x) \times g(x) \bmod m(x) = x^7 + x^6 + 1$. Redoing this in binary arithmetic, we need to compute $(01010111) \times (10000011)$. First, we determine the results of multiplication by powers of x:

$$
\begin{aligned}
(01010111) \times (00000010) &= (10101110) \\
(01010111) \times (00000100) &= (01011100) \oplus (00011011) = (01000111) \\
(01010111) \times (00001000) &= (10001110) \\
(01010111) \times (00010000) &= (00011100) \oplus (00011011) = (00000111) \\
(01010111) \times (00100000) &= (00001110) \\
(01010111) \times (01000000) &= (00011100) \\
(01010111) \times (10000000) &= (00111000)
\end{aligned}
$$

So,

$$
\begin{aligned}
(01010111) \times (10000011) &= (01010111) \times [(00000001) \oplus (00000010) \oplus (10000000)] \\
&= (01010111) \oplus (10101110) \oplus (00111000) = (11000001)
\end{aligned}
$$

which is equivalent to $x^7 + x^6 + 1$.

Using a Generator

- A generator *g* of a finite field F of order *q* (contains *q* elements) is an element whose first *q-1* powers generate all the nonzero elements of F
  - The elements of F consist of 0, g^0, g^1, ..., g^{q-2}
- Consider a field F defined by a polynomial *f(x)*
  - An element *b* contained in F is called a root of the polynomial if *f(b) = 0*
- Finally, it can be shown that a root *g* of an irreducible polynomial is a generator of the finite field defined on that polynomial

Example

the finite field GF(2^3), defined over the irreducible polynomial

$x^3 + x + 1$

Thus, the generator g must satisfy $f(g) = g^3 + g + 1 = 0$.

$g^3 = -g - 1 = g + 1$

We now show that g in fact generates
all of the polynomials of degree less than 3

$$g^4 = g(g^3) = g(g + 1) = g^2 + g$$
$$g^5 = g(g^4) = g(g^2 + g) = g^3 + g^2 = g^2 + g + 1$$
$$g^6 = g(g^5) = g(g^2 + g + 1) = g^3 + g^2 + g = g^2 + g + g + 1 = g^2 + 1$$
$$g^7 = g(g^6) = g(g^2 + 1) = g^3 + g = g + g + 1 = 1 = g^0$$

We see that the powers of g generate all the nonzero polynomials in GF(2^3)

Cont'd

$\boxed{g^k = g^{k \bmod 7} \text{ for any integer } k}$

For example, $g^4 + g^6 = g^{(10 \bmod 7)} = g^3 = g + 1$

The same result is achieved using polynomial arithmetic:

$g^4 = g^2 + g$ and $g^6 = g^2 + 1$

Then, $(g^2 + g) \times (g^2 + 1) = g^4 + g^3 + g^2 + 1$

$(g^4 + g^3 + g^2 + 1) \bmod (g^3 + g + 1)$ by division:

We get a result of $g + 1$

$$
\begin{array}{r}
g \quad + 1 \\
g^3 + g + 1 \,\big/\, \overline{g^4 + g^3 + g^2 + g} \\
\underline{g^4 + \qquad\quad g^2 + g} \\
g^3 \qquad\qquad \\
\underline{g^3 + \qquad\quad g + 1} \\
g + 1
\end{array}
$$

Table 4.9 shows the power representation, as well as the polynomial and binary representations.

Table 4.10 GF(2^3) Arithmetic Using Generator for the Polynomial ($x^3 + x + 1$)

		000	001	010	100	011	110	111	101
	+	0	1	G	g^2	g^3	g^4	g^5	g^6
000	0	0	1	G	g^2	$g + 1$	$g^2 + g$	$g^2 + g + 1$	$g^2 + 1$
001	1	1	0	$g + 1$	$g^2 + 1$	g	$g^2 + g + 1$	$g^2 + g$	g^2
010	g	g	$g + 1$	0	$g^2 + g$	1	g^2	$g^2 + 1$	$g^2 + g + 1$
100	g^2	g^2	$g^2 + 1$	$g^2 + g$	0	$g^2 + g + 1$	g	$g + 1$	1
011	g^3	$g + 1$	g	1	$g^2 + g + 1$	0	$g^2 + 1$	g^2	$g^2 + g$
110	g^4	$g^2 + g$	$g^2 + g + 1$	g^2	g	$g^2 + 1$	0	1	$g + 1$
111	g^5	$g^2 + g + 1$	$g^2 + g$	$g^2 + 1$	$g + 1$	g^2	1	0	g
101	g^6	$g^2 + 1$	g^2	$g^2 + g + 1$	1	$g^2 + g$	$g + 1$	g	0

(a) Addition

		000	001	010	100	011	110	111	101
	×	0	1	G	g^2	g^3	g^4	g^5	g^6
000	0	0	0	0	0	0	0	0	0
001	1	0	1	G	g^2	$g + 1$	$g^2 + g$	$g^2 + g + 1$	$g^2 + 1$
010	g	0	g	g^2	$g + 1$	$g^2 + g$	$g^2 + g + 1$	$g^2 + 1$	1
100	g^2	0	g^2	$g + 1$	$g^2 + g$	$g^2 + g + 1$	$g^2 + 1$	1	g
011	g^3	0	$g + 1$	$g^2 + g$	$g^2 + g + 1$	$g^2 + 1$	1	g	g^2
110	g^4	0	$g^2 + g$	$g^2 + g + 1$	$g^2 + 1$	1	g	g^2	$g + 1$
111	g^5	0	$g^2 + g + 1$	$g^2 + 1$	1	g	g^2	$g + 1$	$g^2 + g$
101	g^6	0	$g^2 + 1$	1	g	g^2	$g + 1$	$g^2 + g$	$g^2 + g + 1$

(b) Multiplication

Table 4.7 Polynomial Arithmetic Modulo $(x^3 + x + 1)$

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

(b) Multiplication

Generator for GF(2^3) using $x^3 + x + 1$

Power Representation	Polynomial Representation	Binary Representation	Decimal (Hex) Representation
0	0	000	0
g^0 (= g^7)	1	001	1
g^1	g	010	2
g^2	g^2	100	4
g^3	$g + 1$	011	3
g^4	$g^2 + g$	110	6
g^5	$g^2 + g + 1$	111	7
g^6	$g^2 + 1$	101	5

Conclusion

- In general, for $GF(2^n)$ with irreducible polynomial $f(x)$, determine $g^n = f(g) - g^n$. Then calculate all of the powers of g from g^{n+1} through g^{2n-2}.
- The elements of the field correspond to the powers of g from g^0 through g^{2n-2} plus the value 0.
- For multiplication of two elements in the field, use the equality $g^k = g^{k \bmod (2n-1)}$ for any integer k.