Chapter 4

Basic Concepts in Number Theory and Finite Fields

Dr. Shin-Ming Cheng

NTUST

CONNECTIVITY LAB

Introduction

- Finite fields
- Increasing importance in cryptography
  - AES, Elliptic Curve, IDEA, Public Key
- Concern operations on “numbers”
  - where what constitutes a “number” and the type of operations varies considerably
- Start with basic number theory concepts

Divisors 除數

› A non-zero number b **divides** a if for some m have $a = mb$ (a, b, m are all integers)
  – b divides into a with no remainder
  – denote as $b|a$
  – b is a **divisor** of a

› Example
  – all of $1,2,3,4,6,8,12,24$ divide 24
  – $13 \mid 182;\ -5 \mid 30;\ 17 \mid 289;\ -3 \mid 33;\ 17 \mid 0$

Properties of Divisibility

- If $a|1$, then $a = \pm 1$.
- If $a|b$ and $b|a$, then $a = \pm b$.
- Any $b \neq 0$ divides 0.
- If $a \mid b$ and $b \mid c$, then $a \mid c$
  - 11 | 66 and 66 | 198, then 11 | 198
- If $b|g$ and $b|h$, then $b|(mg + nh)$ for arbitrary integers m and n
  - $b = 7$; $g = 14$; $h = 63$; $m = 3$; $n = 2$ hence 7|14 and 7|63

Division Algorithm

- If divide a by n get integer quotient q and integer remainder r such that:
  - $a = qn + r$ where $0 <= r < n; q = \lfloor(a/n)\rfloor$
- The remainder r often referred to as a **residue** **餘數**

Greatest Common Divisor (GCD)

- A common problem in number theory
- $\gcd(a, b)$ of a and b is the largest integer that divides evenly into both a and b
  - $\gcd(60,24) = 12$
- Define $\gcd(0, 0) = 0$
- The numbers with no common factors (except 1) are defined as relatively prime 互質
  - $\gcd(8,15) = 1$
    - hence 8 and 15 are relatively prime

Greatest Common Divisor

- Assume $a, b \in Z$, $a \neq 0$ or $b \neq 0$
- **Definition** $d \neq 0$ is a common divisor of a and b if $d \mid a$ and $d \mid b$
- **Definition** The greatest common divisor $d = \gcd(a, b)$ is the largest of the common divisors
  - Divisors of 20: $\pm 1, \pm 2, \pm 4, \pm 5, \pm 10, \pm 20$
  - Divisors of 16: $\pm 1, \pm 2, \pm 4, \pm 8, \pm 16 \Rightarrow \gcd(20, 16) = 4$
- **Proposition** $a \in P$ (positive integer)
  - $\gcd(a, a) = a$, $\gcd(a, 0) = a$
- **Proposition** $a, b \in Z$, $a \neq 0$ or $b \neq 0$
  - $\gcd(a, b) = \gcd(|a|, |b|)$, $\gcd(a, b) = \gcd(b, a)$

Greatest Common Divisor

- **Theorem** $a, b \in Z$, $a \neq 0$ or $b \neq 0$, then $\gcd(a, b) = \gcd(a + kb, b)$ for any $k \in Z$
- **Proof**

  Define
  - A = The set of common divisors of a and b
  - B = The set of common divisors of $a + kb$ and b
  - $A \subset B$:
    - Assume $d \in A$, then $d \mid a$ and $d \mid b$
      - $a = xd$ and $b = yd$ for some $x, y \in Z$
    - Then $a + kb = xd + k(yd) = (x + ky)d \Rightarrow d \mid (a + kb)$.
    - Also $d \mid b$, hence $d \in B$.

Greatest Common Divisor

- $B \subset A$:
  - Assume $c \in B$, then $c \mid (a + kb)$ and $c|b$
    - $a + kb = xc$ and $b = yc$ for some $x, y \in Z$
  - Then $a = xc - kb = xc - k(yc) = (x - ky)c \Rightarrow c \mid a.$
  - Also $c \mid b$, hence $c \in A$.
- Therefore $A = B$, $\gcd(a, b) = \gcd(a + kb, b)$

- **Corollary** $b > 0$, then $\gcd(a, b) = \gcd(b, a \bmod b)$
- **Proof** $\gcd(a, b) = \gcd\left(a - \left\lfloor \frac{a}{b} \right\rfloor \times b, b\right) \overset{\text{[Theorem]}}{=} \underset{\text{[Definition]}}{\gcd(a \bmod b, b)} = \gcd(b, a \bmod b)$ [Proposition]

Example gcd(1970,1066)

$1970 = 1 \times 1066 + 904$	$\gcd(1066, 904)$
$1066 = 1 \times 904 + 162$	$\gcd(904, 162)$
$904 = 5 \times 162 + 94$	$\gcd(162, 94)$
$162 = 1 \times 94 + 68$	$\gcd(94, 68)$
$94 = 1 \times 68 + 26$	$\gcd(68, 26)$
$68 = 2 \times 26 + 16$	$\gcd(26, 16)$
$26 = 1 \times 16 + 10$	$\gcd(16, 10)$
$16 = 1 \times 10 + 6$	$\gcd(10, 6)$
$10 = 1 \times 6 + 4$	$\gcd(6, 4)$
$6 = 1 \times 4 + 2$	$\gcd(4, 2)$
$4 = 2 \times 2 + 0$	$\gcd(2, 0)$

Modular Arithmetic

- Define **modulo operator/模運算** "$a \bmod n$" to be remainder when a is divided by n
  - integer n is called the **modulus**
  - b is called a **residue/餘數** of $a \bmod n$
    - since with integers can always write: $a = qn + b$
    - usually chose smallest positive remainder as residue
    - $0 \le b \le n - 1$
- a and b are **congruent/全等**
  - If $a \bmod n = b \bmod n$
  - $a \equiv b \bmod n$
  - when divided by n, a and b have same remainder
    - $100 = 34 \bmod 11$

Modular Arithmetic Operations

- performs arithmetic with residues
- uses a finite number of values, and loops back from either end
  - $Z_n = \{0, 1, \ldots, (n - 1)\}$
- modular arithmetic is when do addition and multiplication and modulo reduce answer
- can do reduction at any point
  - $a + b \bmod n = [a \bmod n + b \bmod n] \bmod n$

Modular Arithmetic Operations

- $[(a \bmod n) + (b \bmod n)] \bmod n = (a + b) \bmod n$
  - $[(11 \bmod 8) + (15 \bmod 8)] \bmod 8 = 10 \bmod 8 = 2$ $(11 + 15) \bmod 8 = 26 \bmod 8 = 2$
- $[(a \bmod n) - (b \bmod n)] \bmod n = (a - b) \bmod n$
  - $[(11 \bmod 8) - (15 \bmod 8)] \bmod 8 = -4 \bmod 8 = 4$ $(11 - 15) \bmod 8 = -4 \bmod 8 = 4$
- $[(a \bmod n) \times (b \bmod n)] \bmod n = (a \times b) \bmod n$
  - $[(11 \bmod 8) \times (15 \bmod 8)] \bmod 8 = 21 \bmod 8 = 5$ $(11 \times 15) \bmod 8 = 165 \bmod 8 = 5$

Modulo 8 Addition Example

+	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

Modulo 8 Multiplication

×	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

Modular Arithmetic Properties (1/2)

- 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
  - $[w \times (x + y)] \bmod n = [(w \times x) + (w \times y)] \bmod n$

Modular Arithmetic Properties (2/2)

- 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 $w + z = 0 \bmod n$

Euclidean Algorithm 輾轉相除法

- An efficient way to find the $\gcd(a, b)$
- Theorem
  - $\gcd(a, b) = \gcd(b, a \bmod b)$
- Euclidean Algorithm to compute $\gcd(a, b)$ is:

  $Euclid(a, b)$

```
int Euclid(int a, int b){
 if (b==0)
    then return a;
  else
    return Euclid(b, a mod b);
}
```

Euclidean Algorithm

$$
\begin{aligned}
&\gcd(325, 234) \\
&= \gcd(234, 325 \bmod 234) \\
&= \gcd(234, 91) \\
&= \gcd(91, 234 \bmod 91) \\
&= \gcd(91, 52) \\
&= \gcd(52, 91 \bmod 52) \\
&= \gcd(52, 39) \\
&= \gcd(39, 52 \bmod 39) \\
&= \gcd(39, 13) \\
&= \gcd(13, 39 \bmod 13) \\
&= \gcd(13, 0) = 13
\end{aligned}
$$

1	325	234	2
	234	182	
1	91	52	1
	52	39	
3	39	13	
	39		
	0		

Extended GCD Algorithm

- Goal
  - Given $a, b \in Z$
  - Find $x, y \in Z$ such that $ax + by = d = \gcd(a, b)$
    - calculates not only GCD but x and y:
  - Useful for later crypto computations
- $\gcd(a, p) = 1$
  - $b = p$ is a prime number
  - a and p are relatively prime
  - Then x is a **multiplicative inverse** of a in Z_P
    - $ax \equiv 1 \pmod{p}$

Extended GCD Algorithm

- $a = 100,\ b = 35$
  - $100 = 2 \times 35\ +\ 30$
    $35\ = 1 \times 30 +\ 5$
    $30\ = 6 \times 5\ +\ 0$

  - $\gcd(100, 35) = 5$
    $= 35 - 30$
    $= 35 - (100 - 2 \times 35)$
    $= (-1) \times 100 + 3 \times 35$
  - Hence $x = -1,\ y = 3$

Extended GCD Algorithm

- **Theorem** Given $a, b \in Z$,there exit $x, y \in Z$ for the linear combination $ax + by = \gcd(a, b)$.
- Proof
  - Take $r_0 = a = a \times 1_{[=x_0]} + b \times 0_{[=y_0]} = ax_0 + by_0$
  - Take $r_1 = b = a \times 0_{[=x_1]} + b \times 1_{[=y_1]} = ax_1 + by_1$
  - For $i > 0,$ let $q_{i+1} = \lfloor r_{i+1}/r_i \rfloor$; $x_{i+1} = x_{i-1} - x_i q_{i+1}$; $r_{i+1} = r_{i\text{-}1} - r_i\, q_{i+1}$; $y_{i+1} = y_{i-1} - y_i\, q_{i+1}$

Extended GCD Algorithm

- Assume $r_{i\text{-}1} = ax_{i-1} + by_{i\text{ -}1}$ and $r_i = ax_i + by_i$
- Then $r_{i+1} = r_{i-1} - r_i q_{i+1} = (ax_{i-1} + by_{i-1}) - (ax_i + by_i)q_{i+1} = a(x_{i-1} + x_i q_{i+1}) + b(y_{i-1} -$

Notation

- $\boldsymbol{Z} = \{\ \dots, -3, -2, -1, 0, 1, 2, 3, \dots\}$ of integers
- $\boldsymbol{Z}_n = \{0, 1, 2, \dots, n-1\}$
- $\boldsymbol{Z}_n^* = \{1,2,3, \dots, n-1\}$
- $\boldsymbol{N} = \{0, 1, 2, 3, \dots\}$ of non-negative integers
- $\boldsymbol{P}\ = \{1, 2, 3, \dots\}$ of positive integers
- $\boldsymbol{Q}$: The set of rational numbers
- $\boldsymbol{R}$: The set of real numbers
- $\boldsymbol{C}$: The set of complex numbers
- $\boldsymbol{Q}^*, \boldsymbol{R}^*, \boldsymbol{C}^*$: The set of non-zero rational, real, complex numbers

Basics of Abstract Algebra

- **Group** **群**
- Ring 環
- Field 體

Group

- **Definition** A group $(G, \cdot)$ is a set G with an operation $\cdot$, such that the following conditions are satisfied:
  - Closure: $a \cdot b \in G$ for all $a, b \in G$
  - Associativity: $a \cdot (b \cdot c) = (a \cdot b) \cdot \mathrm{c}$ for all $a, b, c \in G$
  - Identity: there is an element $e \in G$ such that $a = a \cdot e = e \cdot a$ for each $a \in G$
  - Inverse: for each $a \in G$, there is an element $b \in G$ such that $a \cdot b = b \cdot a = e$
  - if commutative $a \cdot b = b \cdot a$
    - then forms an abelian group

Group

- Each of the following sets with the specified operation is a group
  - $\boldsymbol{Z}, \boldsymbol{Q}, \boldsymbol{R}, \boldsymbol{C}$ with + (addition)
  - $\boldsymbol{Q}^*, \boldsymbol{R}^*, \boldsymbol{C}^*$ with × (multiplication)
  - $5\boldsymbol{Z} = \{5a | a \in Z\}$ with +
  - $\{1, -1\}$ with ×
  - $\boldsymbol{Z}_6 = \{0, 1, 2, 3, 4, 5\}$ with + modulo 6
  - $D(\boldsymbol{R}) = \{ f \mid f$ is a differentiable function on $\boldsymbol{R} \}$ with +

Group

- None of the following sets with the specified operation is a group
  - $\boldsymbol{Z}_7 = \{0, 1, 2, 3, 4, 5, 6\}$ with $+$ but no modulo
    - not closed
  - $\boldsymbol{P}$ with $+$
    - no identity
  - $\boldsymbol{Z}$ with $-$
    - not associative
  - $2\boldsymbol{Z} + 1 = \{\, 2a + 1 \mid a \in \boldsymbol{Z} \,\}$ with $\times$
    - no inverse

Group

- Proposition
- The identity e of G is unique

  Proof
  - Assume e_1 and e_2 are identity
  - Then $e_1 = e_1 * e_2$ ($\because$ e_2 is an identity)

    $= e_2$ ($\because e_1$ is an identity)
- The inverse b of each $a \in G$ is unique

  Proof
  - Assume b and c are inverse of a
  - Then $b = b * e = b * (a * c) = (b * a) * c = e * c = c$
  - Denoted as a^{-1}

Group

- Proposition
  - $(a^{-1})^{-1} = a$ for all $a \in G$
  - $(a * b)^{-1} = b^{-1} * a^{-1}$ for all $a, b \in G$

- For all $a, b, c \in \mathrm{G}$
  - $a * x = b$ and $y * a = b$ have unique solutions in G
    - $a^{-1} * a * x = x = a^{-1} * b$
    - $y * a * a^{-1} = y = b * a^{-1}$
  - $a * b = a * c \Rightarrow b = c$ and $a * b = c * b \Rightarrow \mathrm{a} = \mathrm{c}$

Cyclic Group

- **Definition** A group $(G, \cdot)$ is **cyclic** if there exists a generator $g \in G$ such that every $a \in G$ is of the form $a = g \cdot \ldots \cdot g$ (n copies) for some $n \in Z$
- **Example**
  - $(\boldsymbol{Z}, +)$ is cyclic with generators 1 and -1
  - $(\boldsymbol{Z}_7^*, \otimes)$ is cyclic: $\{1_{=3^0=3^6}, 2_{=3^2}, 3_{=3^1}, 4_{=3^4}, 5_{=3^5}, 6_{=3^3}\}$
  - $(\boldsymbol{Z}_9^*, \otimes)$ is cyclic with generators 2 and 5

Cyclic Group

- Define exponentiation as repeated application of operator
  - $a^3 = a \cdot a \cdot a$
- Let identity be: $e = a^0$
- A group is cyclic if every element is a power of some fixed element
  - $b = a^k$ for some a and every b in group
- a is said to be a generator of the group

Ring

- **Definition** A ring $(R, +, \times)$ is a set R with two binary operations $+$ and $\times$ such that
  - $(R, +)$ is an abelian group/交換群
  - Closed under $\times$: $a \times b \in R$ for all $a, b \in R$
  - Associative under $\times$:

    $$a \times (b \times c) = (a \times b) \times c$$

    for all $a, b, c \in R$
  - Distributive laws :

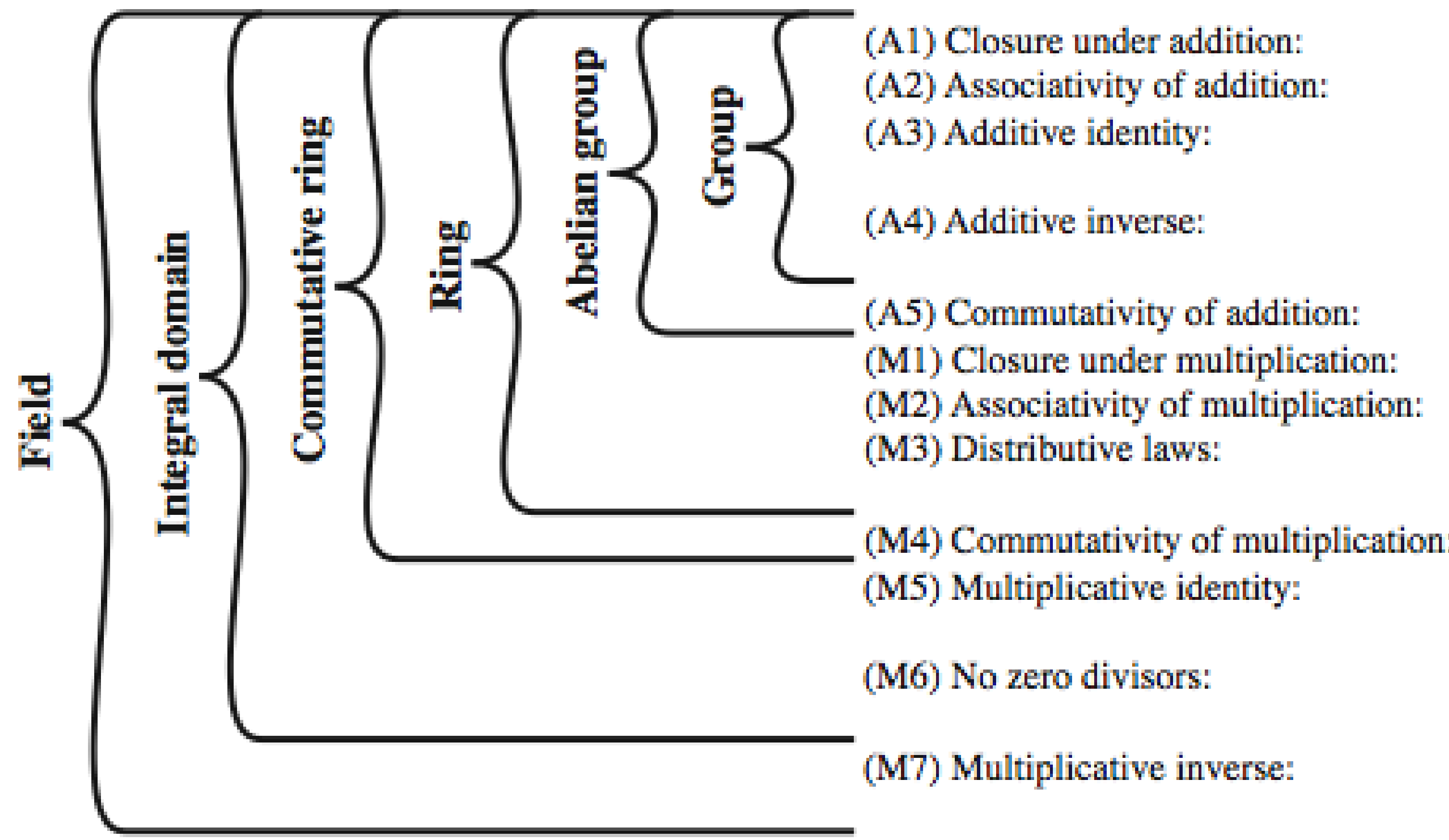
    $$a \times (b + c) = a \times b + a \times c$$
    $$(a + b) \times c = a \times c + b \times c$$

    for all $a, b, c \in R$

Field

- **Definition** A ring R is a field if every nonzero $a \in R$ has an inverse a^{-1}
- **Example**
  - $\boldsymbol{Q}, \boldsymbol{R}, \boldsymbol{C}$ are fields
  - $\boldsymbol{Z}_p$ with prime p is a field
    - also denoted as $\boldsymbol{F}_p$ or $GF(p)$, Galois field of order p
  - $GF(2^8)$ is used in AES
- **Example**
  - $\boldsymbol{Z}$ is not a field, since $2^{-1} \notin \boldsymbol{Z}$

Group, Ring, Field



Finite (Galois) Fields

- Évariste Galois (1811–1832)
  - French mathematician
  - Died from wounds suffered in a duel
- finite fields play a key role in cryptography
  - show number of elements in a finite field **must** be a power of a prime p^n
- Galois fields denoted $GF(p^n)$
- in particular often use the fields:
  - $GF(p)$
  - $GF(2^n)$

Galois Fields $GF(p)$

- $GF(p)$ is the set of integers $\{0,1, \dots, p-1\}$ with arithmetic operations modulo prime p
- these form a finite field
  - since have multiplicative inverses
  - find inverse with Extended Euclidean algorithm
- hence arithmetic is "well-behaved" and can do addition, subtraction, multiplication, and division without leaving the field $GF(p)$

$GF(7)$ Multiplication Example

$\times$	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

Polynomial Arithmetic

- Can compute using polynomials

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

  - not interested in any specific value of x
  - known as the indeterminate
- Several alternatives available
  - ordinary polynomial arithmetic
  - poly arithmetic with coefficients mod p
    - Coefficients are in $GF(p)$
  - poly arithmetic with coefficients mod p and polynomials $\bmod m(x)$ whose highest power is some integer n

Ordinary Polynomial Arithmetic

- Add or subtract corresponding coefficients
- Multiply all terms by each other
- Let $f(x) = x^3 + x^2 + 2$ and $g(x) = x^2 - x + 1$

$$f(x) + g(x) = x^3 + 2x^2 - x + 3$$
$$f(x) - g(x) = x^3 + x + 1$$
$$f(x) \times g(x) = x^5 + 3x^2 - 2x + 2$$

Polynomial Arithmetic with Modulo Coefficients

- When computing value of each coefficient do calculation modulo some value
  - forms a polynomial ring
- Could be modulo any prime
- We are most interested in $\bmod 2$
  - all coefficients are 0 or 1
  - let $f(x) = x^3 + x^2$ and $g(x) = x^2 + x + 1$

$$f(x) + g(x) = x^3 + x + 1$$
$$f(x) \times g(x) = x^5 + x^2$$

Polynomial Division

- can write any polynomial 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 say $g(x)$ divides $f(x)$
- if $g(x)$ has no divisors other than itself and 1 say it is irreducible (or prime) polynomial
- arithmetic modulo an irreducible polynomial forms a field

Polynomial GCD

› can find greatest common divisor for polys

– $c(x) = \gcd(a(x), b(x))$ if $c(x)$ is the poly of greatest degree which divides both $a(x)$, $b(x)$

› can find greatest common divisor for polys

– can adapt Euclid's Algorithm to find it

```
Euclid(a(x), b(x))
    if (b(x) = 0) then return a(x);
    else return
    Euclid(b(x), a(x) mod b(x));
```

› all foundation for polynomial fields as see next

Modular Polynomial Arithmetic

- Compute in field $GF(2^n)$
  - polynomials with coefficients modulo 2
  - whose degree is less than n
  - hence must reduce modulo an irreducible poly of degree n (for multiplication only)
- form a finite field
- can always find an inverse
  - can extend Euclid's Inverse algorithm to find
- Motivation
  - 8 bits: 256 is not prime (251 is)

Example $GF(2^3)$

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

(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	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

(b) Multiplication

	×	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	$x+1$

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

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

  - Each a_i takes on a value in the set $\{0,1,\ldots,p-1\}$.
  - There are a total of p^n different polynomials in S
- For $p = 3$ and $n = 2$, the $3^2 = 9$ polynomial S in the set are
  - $0, 1, 2, x, x+1, x+2, 2x, 2x+1, 2x+2$
- For $p = 2$ and $n = 3$, the $2^3 = 9$ polynomial S in the set are
  - $0, 1, x, x+1, x^2, x^2+1, x^2+x, x^2+x+1$

Finding the Multiplicative Inverse

- Extended GCD
  - 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 $d(x) = 1$, there $w(x)$ is the multiplicative inverse of $b(x)$ modulo a(x)

Computational Considerations

- Since coefficients are 0 or 1, can represent any such polynomial as a bit string
- addition becomes XOR of these bit strings
- multiplication is shift and XOR
  - long-hand multiplication
- modulo reduction done by repeatedly substituting highest power with remainder of irreducible poly (also $shift$ and XOR)
  - if in $GF(2^n)$ then irreducible poly $g(x)$ has highest term x^n , and if compute x^n mod $g(x)$ answer is $g(x) - x^n$

Computational Example

- $GF_8 = GF(2^3)$ (x^2+1) is 101_2 and (x^2+x+1) is 111_2
- addition is
  - $(x^2+1) + (x^2+x+1) = x$
  - $101\ XOR\ 111 = 010_2$
- multiplication is
  - $(x+1) \times (x^2+1) = x\,(x^2+1) + 1(x^2+1)$
    $= x^3+x+x^2+1 = x^3+x^2+x+1$
  - $011 \times 101 = (101) << 1\ XOR\ (101) << 0 =$
    $1010\ XOR\ 101 = 1111_2$
- polynomial modulo reduction (get $q(x)$ and $r(x)$) is
  - $(x^3+x^2+x+1) \bmod (x^3+x+1) = 1(x^3+x+1) + (x^2) = x^2$
  - $1111 \bmod 1011 = 1111\ XOR\ 1011 = 0100_2$

Galois Fields

- Irreducible Polynomials for the Modulus

n=1	e
10	1
11	1

n=2	e
111	3

n=3	e
1011	7
1101	7

n=4	e
10011	15
11001	15
11111	5

n=5	e
100101	31
101001	31
101111	31
110111	31
111011	31
111101	31

n=6	e
1000011	63
1001001	9
1010111	21
1011011	63
1100001	63
1100111	63
1101101	63
1110011	63
1110101	21

n=7	e
10000011	127
10001001	127
10001111	127
10010001	127
10011101	127
10100111	127
10101011	127
10111001	127
10111111	127
11000001	127
11001011	127
11010011	127
11010101	127
11101111	127
11110001	127
11110111	127
11111101	127

n=8	e
100011011	51
100011101	255
100101011	255
100101101	255
100111001	17
100111111	85
101001101	255
101011111	255
101100011	255
101100101	255
101101001	255
101110001	255
101110111	85
101111011	85
110000111	255
110001011	85
110001101	255
1100111111	51
110100011	85
110101001	255
110110001	51
110111101	85
111000011	255
111001111	255
111010111	17
111011101	85
111100111	255
111110011	51
111110101	255
111111001	85