# Chapter 4
# Basic Concepts in Number Theory and Finite Fields



## Divisibility

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

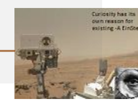
The positive divisors of 24 are 1, 2, 3, 4, 6, 8, 12, and 24
13 | 182; - 5 | 30; 17 | 289; - 3 | 33; 17 | 0

## Properties of Divisibility

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

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

11 | 66 and 66 | 198 = 11 | 198



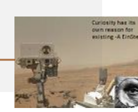



## Properties of Divisibility

- To see this last point, note that:
  - If $b$ / $g$ , then $g$ is of the form $g = b * g_1$ for some integer $g_1$
  - If $b$ / $h$ , 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 $mg + nh$

$b$ = 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)).

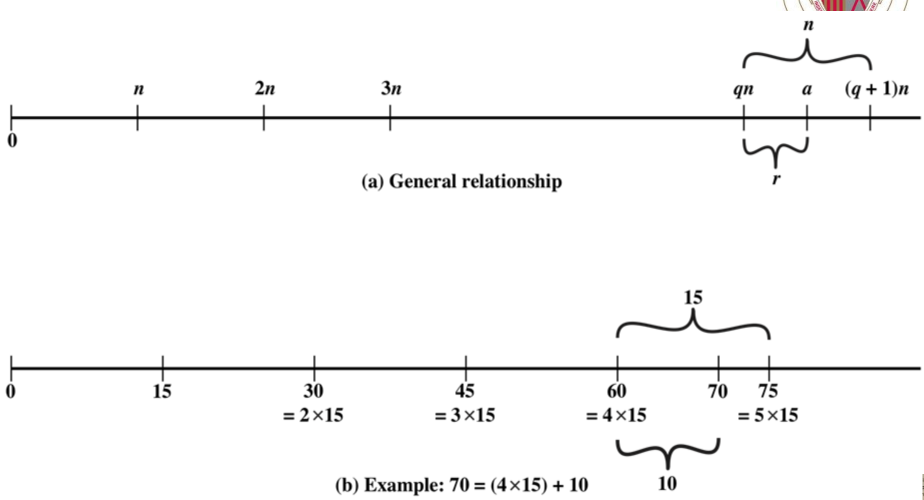


# Division Algorithm

- 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:

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



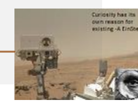



(a) General relationship

(b) Example: 70 = (4×15) + 10

# Euclidean Algorithm

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






# 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:

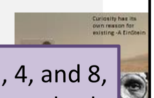
$$\gcd(a,b) = \max[k, \text{ such that } k \mid a \text{ and } k \mid b]$$

# 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 |)*

gcd(60, 24) = gcd(60, - 24) = 12

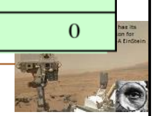
- Also, because all nonzero integers divide 0, we have *gcd(a,0) = | a |*
- We stated that two integers *a* and *b* are relatively prime if their only common positive integer factor is 1; this is equivalent to saying that *a* and *b* are relatively prime if *gcd(a,b) = 1*




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 |



**GCD(1160718174, 316258250) = 1078**

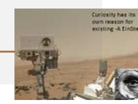
# Modular Arithmetic

- 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:*

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

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

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






# Modular Arithmetic

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

73 = 4 (mod 23); 21 = - 9 (mod 10)

# Properties of Congruences

- Congruences have the following properties:
  1. $a = b \pmod{n}$ if $n (a – b)$
  2. $a = b \pmod{n}$ implies $b = a \pmod{n}$
  3. $a = b \pmod{n}$ and $b = c \pmod{n}$ imply $a = c \pmod{n}$
- 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 $n$)

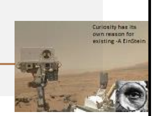

23 = 8 (mod 5) because 23 - 8 = 15 = 5 * 3
- 11 = 5 (mod 8) because - 11 - 5 = - 16 = 8 * (- 2)
81 = 0 (mod 27) because 81 - 0 = 81 = 27 * 3



# Modular Arithmetic

- Modular arithmetic exhibits the following properties:
  1. $[(a \bmod n) + (b \bmod n)] \bmod n = (a + b) \bmod n$
  2. $[(a \bmod n) - (b \bmod n)] \bmod n = (a - b) \bmod n$
  3. $[(a \bmod n) * (b \bmod n)] \bmod n = (a * b) \bmod n$
- We demonstrate the first property:
  - Define ($a$ mod $n$) = $r_a$ and ($b$ 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:

$$\begin{aligned}(a + b) \bmod n &= (ra + jn + rb + kn) \bmod n\\ &= (ra + rb + (k + j)n) \bmod n\\ &= (ra + rb) \bmod n\\ &= [(a \bmod n) + (b \bmod n)] \bmod n\end{aligned}$$



# Remaining Properties:

- Examples of the three remaining properties:

11 mod 8 = 3; 15 mod 8 = 7

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

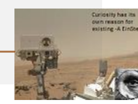
(11 + 15) mod 8 = 26 mod 8 = 2

[(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






# Table 4.2(a) 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 |

# Table 4.2(b)
# Multiplication 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 |




# Additive/Multiplicative Inverses 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 |

**W+ (-w)) = 0 mod 8**
**W * W^-1 = 1 mod 8**

# Properties of Modular Arithmetic for Integers in $Z_n$

| Property | Expression |
|---|---|
| Commutative Laws | $(w + x) \bmod n = (x + w) \bmod n$<br>$(w \times x) \bmod n = (x \times w) \bmod n$ |
| Associative Laws | $[(w + x) + y] \bmod n = [w + (x + y)] \bmod n$<br>$[(w \times x) \times y] \bmod n = [w \times (x \times y)] \bmod n$ |
| Distributive Law | $[w \times (x + y)] \bmod n = [(w \times x) + (w \times y)] \bmod n$ |
| Identities | $(0 + w) \bmod n = w \bmod n$<br>$(1 \times w) \bmod n = w \bmod n$ |
| Additive Inverse $(-w)$ | For each $w \in Z_n$, there exists a $z$ such that $w + z \equiv 0 \bmod n$ |



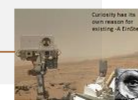
# Extended Euclidean Algorithm Example

| $i$ | $r_i$ | $q_i$ | $x_i$ | $Y_i$ |
|---|---|---|---|---|
| –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 set of elements with a binary operation denoted by • that associates to each ordered pair $(a,b)$ of elements in $G$ an element $(a \bullet b)$ in $G$, such that the following axioms are obeyed:
  - (A1) Closure:
    - If $a$ and $b$ belong to $G$, then $a \bullet b$ is also in $G$
  - (A2) Associative:
    - $a \bullet (b \bullet c) = (a \bullet b) \bullet c$ for all $a, b, c$ in $G$
  - (A3) Identity element:
    - There is an element $e$ in $G$ such that $a \bullet e = e \bullet a = a$ for all $a$ in $G$
  - (A4) Inverse element:
    - For each $a$ in $G$, there is an element $a$ in $G$ such that $a \bullet a = a \bullet a = e$
  - (A5) Commutative:
    - $a \bullet b = b \bullet a$ for all $a, b$ in $G$






# 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
- 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 , + , * }, 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.)

- 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, +,* }, 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 $aa^{-1} = (a^{-1})a = 1$

- In essence, 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

**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 $S$

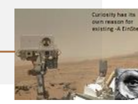
(M6) No zero divisors: If $a, b$ in $S$ and $ab = 0$, then either $a = 0$ or $b = 0$

**Group**

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

# Finite Fields of the Form GF($p$)

- Finite fields play a crucial role in many cryptographic algorithms
- It can be shown that the order of a finite field must be a power of a prime $p^n$, where $n$ is a positive integer
  - The only positive integers that are divisors of $p$ are $p$ and 1
- The finite field of order $p^n$ is generally written GF($p^n$)
  - GF stands for Galois field, in honor of the mathematician who first studied finite fields





# Arithmetic in GF(7)

| + | 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

# Arithmetic in GF(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




# Arithmetic in GF(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

# GF(p)

1. GF($p$) consists of $p$ elements
2. The binary operations + and * 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
3. 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:

- Ordinary polynomial arithmetic, using the basic rules of algebra
- Polynomial arithmetic in which the arithmetic on the coefficients is performed modulo $p$; that is, the coefficients are in GF($p$ )
- 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 $n$

# Ordinary Polynomial Arithmetic Example

As an example:

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

Then:

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

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

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


Figures 4.3a through 4.3c show the manual calculations



$$\begin{array}{r} x^3 + x^2 \qquad + 2 \\ + \; (x^2 - x + 1) \\ \hline x^3 + 2x^2 - x + 3 \end{array}$$

(a) Addition

$$\begin{array}{r} x^3 + x^2 \qquad + 2 \\ - \; (x^2 - x + 1) \\ \hline x^3 \qquad + x + 1 \end{array}$$

(b) Subtraction

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

(c) Multiplication

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

(d) Division


Figure 4.3 Examples of Polynomial Arithmetic

# Polynomial Arithmetic With Coefficients in $Z_p$

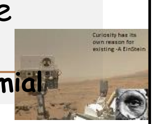
- If each distinct polynomial is considered to be an element of the set, then that set is a ring
- When polynomial arithmetic is performed on polynomials over a field, then division is possible
  - Note: this does not mean that *exact division* is possible
- If we attempt to perform polynomial division over a coefficient set that is not a field, we find that division is not always defined
  - Even if the coefficient set is a field, polynomial division is not necessarily exact
  - With the understanding that remainders are allowed, we can say that polynomial division is possible if the coefficient set is a field




# Polynomial Division

- We can write any polynomial in the form:

  $f(x) = q(x)\, g(x) + r(x)$
  - $r(x)$ can be interpreted as being a remainder
  - So $r(x) = f(x) \bmod g(x)$
- If there is no remainder we can say $g(x)$ **divides** $f(x)$
  - Written as $g(x) \mid f(x)$
  - We can say that $g(x)$ is a **factor** of $f(x)$
  - Or $g(x)$ is a **divisor** of $f(x)$
- A polynomial $f(x)$ over a field $F$ is called **irreducible** 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 $f(x)$
  - An irreducible polynomial is also called a **prime polynomial**



# Example of Polynomial Arithmetic Over GF(2)

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

(a) Addition

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

(b) Subtraction

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

(c) Multiplication

$$\begin{array}{r|l} & x^4 + 1 \\ \hline x^3 + x + 1 & x^7 + x^5 + x^4 + x^3 + x + 1 \\ & x^7 + x^5 + x^4 \\ \hline & x^3 + x + 1 \\ & x^3 + x + 1 \\ \hline \end{array}$$

(d) Division



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

# Arithmetic in GF($2^3$)

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



# Arithmetic in GF($2^3$)

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

# Arithmetic in GF($2^3$)

| $w$ | $-w$ | $w^{-1}$ |
|---|---|---|
| 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



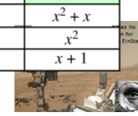

# Polynomial Arithmetic Modulo ($x^3 + x + 1$)

| | + | 000<br>0 | 001<br>1 | 010<br>$x$ | 011<br>$x+1$ | 100<br>$x^2$ | 101<br>$x^2+1$ | 110<br>$x^2+x$ | 111<br>$x^2+x+1$ |
|---|---|---|---|---|---|---|---|---|---|
| 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<br>0 | 001<br>1 | 010<br>$x$ | 011<br>$x+1$ | 100<br>$x^2$ | 101<br>$x^2+1$ | 110<br>$x^2+x$ | 111<br>$x^2+x+1$ |
|---|---|---|---|---|---|---|---|---|---|
| 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



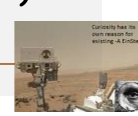
## Extended Euclid $[(x^8 + x^4 + x^3 + x + 1), (x^7 + x + 1)]$

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



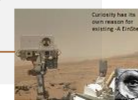
## Computational Considerations

- Since coefficients are 0 or 1, they can represent any such polynomial as a bit string
- Addition becomes XOR of these bit strings
- Multiplication is shift and XOR
  - cf long-hand multiplication
- Modulo reduction is done by repeatedly substituting highest power with remainder of irreducible polynomial (also shift and XOR)



# 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 $fx$
  - 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





# 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 |

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

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



# Summary

- 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($2^n$)