# Module 3 :
# **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 $a \mid 1$, 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 $a \mid c$

  $11 \mid 66$ 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 $mg + nh$

$b = 7$; $g = 14$; $h = 63$; $m = 3$; $n = 2$
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:

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

# Example

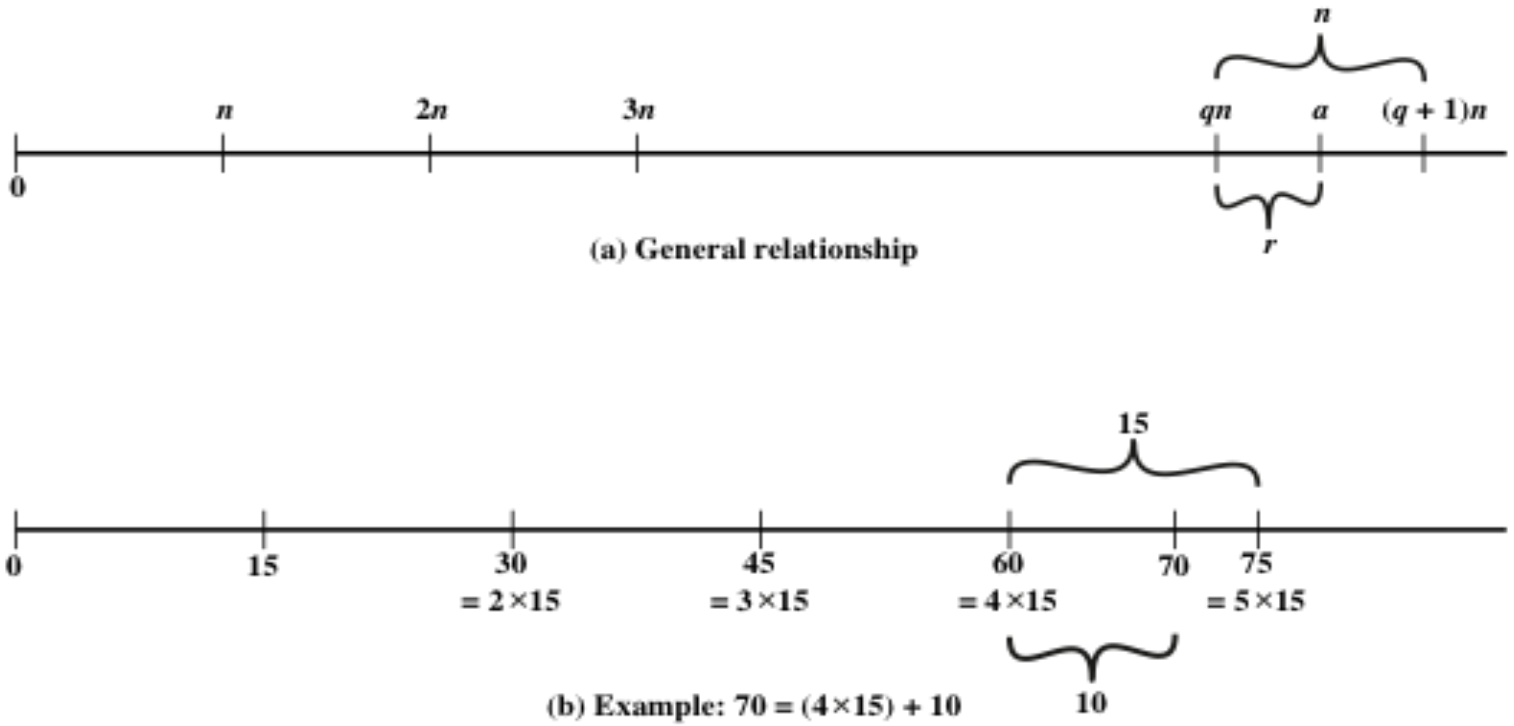



**Figure 2.1 The Relationship $a = qn + r;\ 0 \leq r < n$**

# 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

# 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* |)

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

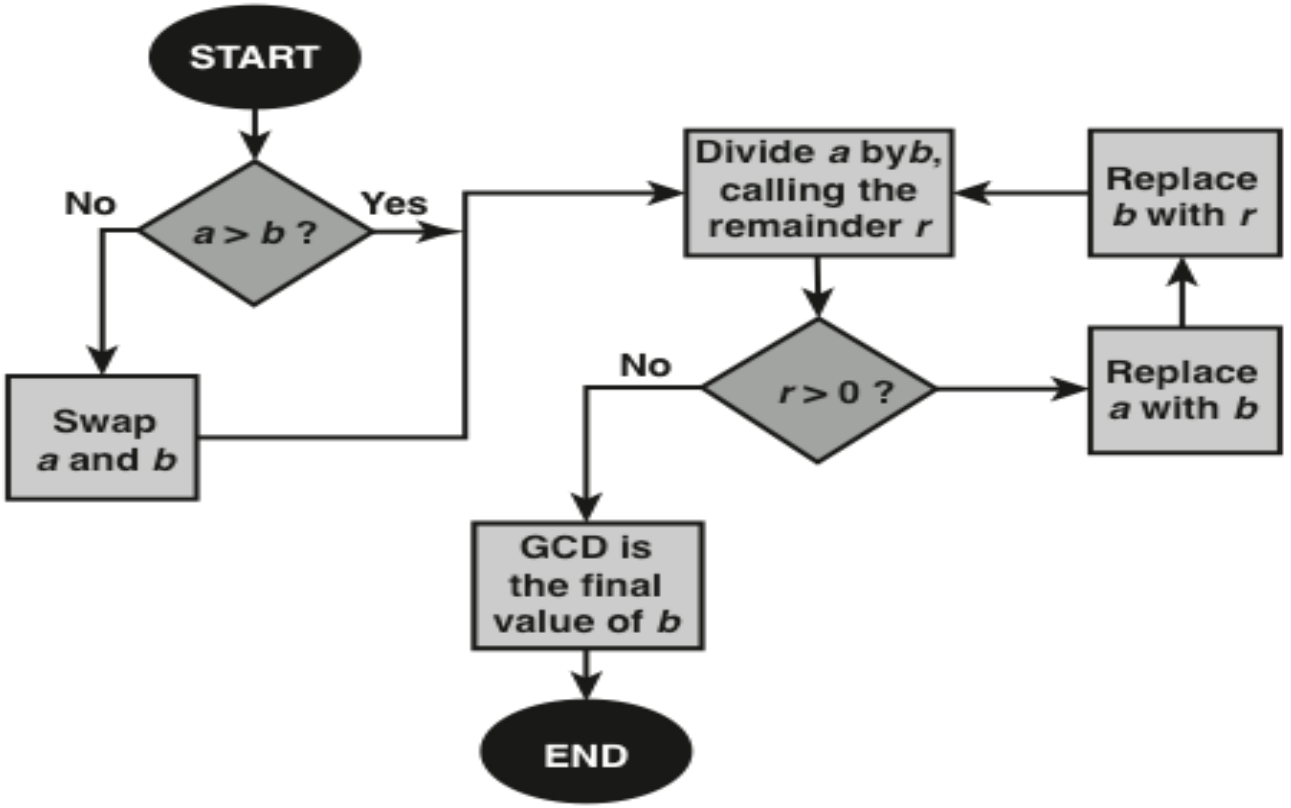



**Figure 2.2 Euclidean Algorithm**

# Euclidean Algorithm - Example

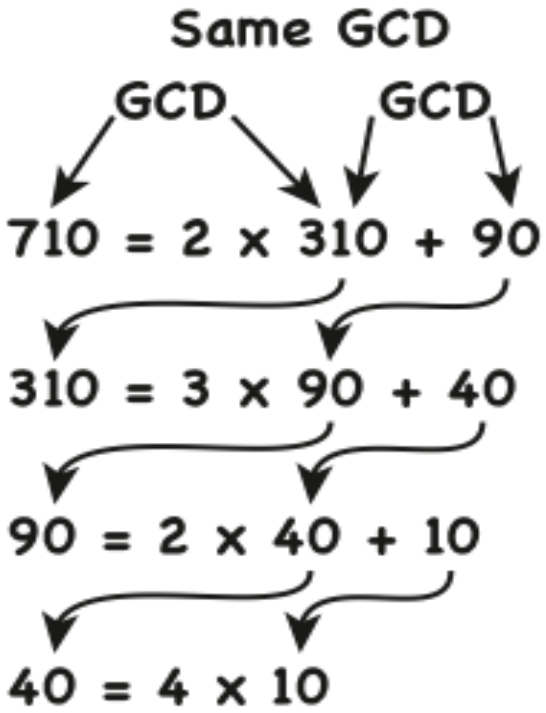



**Figure 2.3 Euclidean Algorithm Example: gcd(710, 310)**

# Euclidean Algorithm

- an efficient way to find the GCD(a,b)
- uses theorem that:
  - GCD(a,b) = GCD(b, a mod b)
- Euclidean Algorithm to compute GCD(a,b) is:
  - EUCLID(a,b)
  - 1. A = a; B = b
  - 2. if B = 0 return  A = gcd(a, b)
  - 3. R = A mod B
  - 4. A = B
  - 5. B = R
  - 6. goto 2

# Example GCD(1970,1066)

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

# Example

- GCD(270,192)
- Answer – 6
- GCD(168, 180)
- Answer – 12
- GCD(1424, 3084)

# Euclidean Algorithm Example

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

# Modular Arithmetic

- is 'clock arithmetic'
- uses a finite number of values, and loops back from either end
- modular arithmetic is
  - when doing addition & multiplication and modulo reducing the answer
  - when reducing, we "usually" want to find the **positive** remainder after dividing by the modulus.
- we can do reduction at any point, i.e.
  - a+b mod n = [a mod n + b mod n] mod n
    - e.g. 11 mod 7 = [8 mod 7 + 3 mod 7] mod n = [1 + 3] mod 7 = 4
  - a-b mod n = [a mod n - b mod n] mod n
  - (a x b) mod n = [a mod n x b mod n] mod n

# 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:*

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

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

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 $a = b \pmod{n}$[2]
  - Note that if $a = 0 \pmod{n}$, then $n \mid a$

$73 = 4 \pmod{23}$;  $21 = -9 \pmod{10}$

# Properties of Congruence

- 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 $(a \bmod n) = r_a$ and $(b \bmod n) = r_b$. Then we can write $a = r_a + jn$ for some integer $j$ and $b = r_b + kn$ for some integer $k$
  - Then:

$$(a + b) \bmod n = (ra + jn + rb + kn) \bmod n$$
$$= (ra + rb + (k + j)n) \bmod n$$
$$= (ra + rb) \bmod n$$
$$= [(a \bmod n) + (b \bmod n)] \bmod n$$

# 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

# Example

- Exponentiation is performed by repeated multiplication, as in ordinary arithmetic.
- Finding $11^7$ mod 13
  - $11^2$ mod 13 = 4 and so $11^2 \equiv 4$ mod 13
  - i.e. $11^4 \equiv 4^2$ mod 13. But $4^2$ mod 13 = 3 i.e. $4^2$ mod 13 $\equiv$ 3 mod13
  - i.e $11^7 \equiv 11 \times 4 \times 3 \equiv 132 \equiv 2$ mod 13

# Modular arithmetic properties…

- can do modular arithmetic with any group of integers:
  - viz. $Z_n = \{0, 1, \ldots, n-1\}$
- Equivalence class
  - The EC of an integer **a** is the set of all those numbers which are congruent to **a modulo n** i.e.
- If $a = qn + r$, with $0 \leq r < n$, then
  - $a \equiv r \bmod n$.
  - Therefore, each integer a in Z is ***≡ modulo n*** to a unique integer between 0 and n-1 – called the least residue of **a modulo n**.
  - Are **a** and **r** in the same equivalence class or different ?

# Equivalence Classes - illustrations

- The EC of [0], [1], [2],…..[n-1] is
  - [r] = {a: a is an integer, a ≡ r mod n}
  - here, r is used to represent the residue class
  - each integer in $Z_n$ represents a residue class of itself.
- Example: the EC (residue classes ) of the least residues 0, 1, 2, 3 modulo 4 represented by [0], [1], [2], [3] respectively are
  - [0] ≡ {……-16,-12,-8,-4, 0, 4, 8, 12, 16, 20,….}
  - [1] ≡ {…..-15, -11, -7, -3, 1, 5, 9, 13, 17,…..}
  - [2] ≡ {….. -18 , -14,-10, -6, -2, 2,6,10,14, …..}
  - [3] ≡ {…..-13, -9, -5, -1, 3, 7, 11, 15, 19, …..}
- The EC is represented by the least residue.

# The integers modulo n

- def: The integers modulo n i.e. $Z_n$ is the set of (equivalence classes of) integers {0,1,2,…..n-1}.
- All the operations in $Z_n$ viz.
  - multiplication, addition and subtraction are performed modulo n.
- e.g. $Z_{25}$ = {0,1,2,3, ……24}. Then,
  - 6+14 = ? in $Z_{25}$
  - 15+35 = ? in $Z_{25}$
  - 14+14 = ? in $Z_{25}$
  - 20+32 = ? in $Z_{25}$
- e.g. $Z_{49}$ = {0,1,2,3,…48}. Then
  - 21+23 = ? in $Z_{49}$
  - 35 + 35 = ? in $Z_{49}$

# Arithmetic Modulo 8

- The additive inverse of a number a in modular arithmetic is the integer y such that x + y = 0 mod n.
- e.g. addition arithmetic modulo 8 is as shown in the table.

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

# Multiplication Modulo 8

- The multiplicative inverse of a number a is a number b such that a * b = 1 mod n.
  - if exists, it is unique
- e.g the table shows the multiplication modulo 8
- unlike additive inverse, the multiplicative inverse of a number may not exist e.g.
  - what is the multiplicative inverse of 4 in modulo 8 ?

| x | 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 |

# 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 $w + z \equiv 0 \bmod n$ |

(This table can be found on page 38 in the textbook)

# Finding Inverses – Extended Euclidean algorithm

**EXTENDED_EUCLID(*m*, *b*)**

**1.** (A1, A2, A3)=(1, 0, *m*);
(B1, B2, B3)=(0, 1, *b*)

**2.** **if** B3 = 0
**return** A3 = gcd(*m*, *b*); no inverse

**3.** **if** B3 = 1
**return** B3 = gcd(*m*, *b*); B2 = $b^{-1}$ mod *m*

**4.** Q = A3 div B3

**5.** (T1, T2, T3)=(A1 – Q B1, A2 – Q B2, A3 – Q B3)

**6.** (A1, A2, A3)=(B1, B2, B3)

**7.** (B1, B2, B3)=(T1, T2, T3)

**8.** **goto** 2

# Inverse of 17 in GF(29)

i.e. calling Extended_Euclid(29, 17)

| Q | A1 | A2 | A3 | B1 | B2 | B3 |
|---|---|---|---|---|---|---|
| — | 1 | 0 | 29 | 0 | 1 | 17 |
| 1 | 0 | 1 | 17 | 1 | –1 | 12 |
| 1 | 1 | –1 | 12 | –1 | 2 | 5 |
| 2 | –1 | 2 | 5 | 3 | –5 | 2 |
| 2 | 3 | –5 | 2 | -7 | 12 | 1 |

# Inverse of 17 in GF(29)

i.e. calling Extended_Euclid(29, 17)

| Q | A1 | A2 | A3 | B1 | B2 | B3 |
|---|---|---|---|---|---|---|
| — | 1 | 0 | 29 | 0 | 1 | 17 |
| 1 | 0 | 1 | 17 | 1 | –1 | 12 |
| 1 | 1 | –1 | 12 | –1 | 2 | 5 |
| 2 | –1 | 2 | 5 | 3 | –5 | 2 |
| 2 | 3 | –5 | 2 | -7 | 12 | 1 |

# Inverse of 37 in GF(49)

i.e. calling Extended_Euclid(49, 37)

| Q | A1 | A2 | A3 | B1 | B2 | B3 |
|---|---|---|---|---|---|---|
| — | 1 | 0 | 49 | 0 | 1 | 37 |
| 1 | 0 | 1 | 37 | 1 | -1 | 12 |
| 3 | 0 | 1 | 12 | -3 | 4 | 1 |

- Hence $37^{-1} \equiv 4 \bmod 49$ OR $4 = 37^{-1} \bmod 49$

# Inverse of 550 in GF(1759)

i.e. calling Extended_Euclid(1759, 550)

| Q | A1 | A2 | A3 | B1 | B2 | B3 |
|---|---|---|---|---|---|---|
| — | 1 | 0 | 1759 | 0 | 1 | 550 |
| 3 | 0 | 1 | 550 | 1 | –3 | 109 |
| 5 | 1 | –3 | 109 | –5 | 16 | 5 |
| 21 | –5 | 16 | 5 | 106 | –339 | 4 |
| 1 | 106 | –339 | 4 | –111 | 355 | 1 |

# Inverse of 49 in GF(37)

i.e. calling Extended_Euclid(37, 49)

| Q | A1 | A2 | A3 | B1 | B2 | B3 |
|---|---|---|---|---|---|---|
| — | 1 | 0 | 37 | 0 | 1 | 49 |
| 0 | 0 | 1 | 49 | 1 | 0 | 37 |
| 1 | 1 | 0 | 37 | -1 | 1 | 12 |
| 3 | -1 | 1 | 12 | 4 | -3 | 1 |

- Hence $49^{-1} \equiv (-3) \bmod 37$
- But, $-3 \pmod{37} \equiv 34 \pmod{37}$. Hence,
- $34 = 37^{-1} \bmod 49$

# Prime Numbers

- Prime numbers only have divisors of 1 and itself
  - They cannot be written as a product of other numbers
- Prime numbers are central to number theory
- Any integer a > 1 can be factored in a unique way as

$$a = p1^{a1} * p_2^{a2} * \ldots * p_{p1}^{a1}$$

where $p_1 < p_2 < \ldots < p_t$ are prime numbers and where each $a_i$ is a positive integer

- This is known as the fundamental theorem of arithmetic

# Primes Under 2000

| 2 | 101 | 211 | 307 | 401 | 503 | 601 | 701 | 809 | 907 | 1009 | 1103 | 1201 | 1301 | 1409 | 1511 | 1601 | 1709 | 1801 | 1901 |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| 3 | 103 | 223 | 311 | 409 | 509 | 607 | 709 | 811 | 911 | 1013 | 1109 | 1213 | 1303 | 1423 | 1523 | 1607 | 1721 | 1811 | 1907 |
| 5 | 107 | 227 | 313 | 419 | 521 | 613 | 719 | 821 | 919 | 1019 | 1117 | 1217 | 1307 | 1427 | 1531 | 1609 | 1723 | 1823 | 1913 |
| 7 | 109 | 229 | 317 | 421 | 523 | 617 | 727 | 823 | 929 | 1021 | 1123 | 1223 | 1319 | 1429 | 1543 | 1613 | 1733 | 1831 | 1931 |
| 11 | 113 | 233 | 331 | 431 | 541 | 619 | 733 | 827 | 937 | 1031 | 1129 | 1229 | 1321 | 1433 | 1549 | 1619 | 1741 | 1847 | 1933 |
| 13 | 127 | 239 | 337 | 433 | 547 | 631 | 739 | 829 | 941 | 1033 | 1151 | 1231 | 1327 | 1439 | 1553 | 1621 | 1747 | 1861 | 1949 |
| 17 | 131 | 241 | 347 | 439 | 557 | 641 | 743 | 839 | 947 | 1039 | 1153 | 1237 | 1361 | 1447 | 1559 | 1627 | 1753 | 1867 | 1951 |
| 19 | 137 | 251 | 349 | 443 | 563 | 643 | 751 | 853 | 953 | 1049 | 1163 | 1249 | 1367 | 1451 | 1567 | 1637 | 1759 | 1871 | 1973 |
| 23 | 139 | 257 | 353 | 449 | 569 | 647 | 757 | 857 | 967 | 1051 | 1171 | 1259 | 1373 | 1453 | 1571 | 1657 | 1777 | 1873 | 1979 |
| 29 | 149 | 263 | 359 | 457 | 571 | 653 | 761 | 859 | 971 | 1061 | 1181 | 1277 | 1381 | 1459 | 1579 | 1663 | 1783 | 1877 | 1987 |
| 31 | 151 | 269 | 367 | 461 | 577 | 659 | 769 | 863 | 977 | 1063 | 1187 | 1279 | 1399 | 1471 | 1583 | 1667 | 1787 | 1879 | 1993 |
| 37 | 157 | 271 | 373 | 463 | 587 | 661 | 773 | 877 | 983 | 1069 | 1193 | 1283 |  | 1481 | 1597 | 1669 | 1789 | 1889 | 1997 |
| 41 | 163 | 277 | 379 | 467 | 593 | 673 | 787 | 881 | 991 | 1087 |  | 1289 |  | 1483 |  | 1693 |  |  | 1999 |
| 43 | 167 | 281 | 383 | 479 | 599 | 677 | 797 | 883 | 997 | 1091 |  | 1291 |  | 1487 |  | 1697 |  |  |  |
| 47 | 173 | 283 | 389 | 487 |  | 683 |  | 887 |  | 1093 |  | 1297 |  | 1489 |  | 1699 |  |  |  |
| 53 | 179 | 293 | 397 | 491 |  | 691 |  |  |  | 1097 |  |  |  | 1493 |  |  |  |  |  |
| 59 | 181 |  |  | 499 |  |  |  |  |  |  |  |  |  | 1499 |  |  |  |  |  |
| 61 | 191 |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| 67 | 193 |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| 71 | 197 |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| 73 | 199 |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| 79 |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| 83 |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| 89 |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| 97 |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |

# Prime Factorization

- to **factor** a number n is to write it as a product of other numbers: n=a x b x c
- factoring a number is relatively hard
  - compared to multiplying the factors together to generate the number
- the **prime factorisation** of a number n is
  - when its written as a product of primes
  - if P is a set of prime numbers, then any positive number can be expressed as a = $p_1^{a1} * p_2^{a2} * p_3^{a3} * p_4^{a4}$ i.e.
  - e.g. 91=7 x 13 ; 3600 = $2^4$ x $3^2$ x $5^2$
  - 12 = ?; 18=?
    - 12 = $2^2$ x $3^1$ and 18 = $2^1$ x $3^2$

$$a = \prod_{p \in \mathrm{P}} p^{a_p}$$

# Prime Factorization

- Multiplication of two numbers is equivalent to adding the corresponding exponents:
  - i.e. $k = mn$ if $k_p = m_p + n_p$ for all $p \in P$
  - e.g. while $12 = 2^2 \times 3^1$ and $18 = 2^1 \times 3^2$ then
    - $18 \times 12 = 2^{2+1} \times 3^{1+2} = 216$
- Any integer of the form $p^k$ can be divided
  - only by an integer that is of a lesser or equal power of the same prime number $p^j$ with $j <= k$
  - i.e. $a \mid b$ if $a_p < b_p$ for all p.

# Relatively Prime Numbers & GCD

- Determining the gcd of two positive integers is easy
  - if they are expressed each - as the product of primes
  - e.g. if $300 = 2^2 \times 3^1 \times 5^2$ and $18 = 2 \times 3^2$ then
    - the gcd(300, 18) is given as
      - $= 2^1 \times 3^1 \times 5^0$
- two numbers a,b are relatively prime if have no common divisors apart from 1
  - eg. 8 & 15 are relatively prime since factors of 8 are 1,2,4,8 and of 15 are 1,3,5,15 and 1 is the only common factor

# The Euler Totient function

- def: For $n \geq 1$, let ø(n) denote the number of integers in the interval [1,n] which are relatively prime to n.
- The function ø is called the Euler Totient function.
- Note that, when we are doing arithmetic modulo n
  - the complete set of residues is : 0……n-1, whereas,
  - the reduced set of residues is those numbers (residues) which are relatively prime to n
    - eg for n=10,
      - the complete set of residues is {0,1,2,3,4,5,6,7,8,9}
      - the reduced set of residues is {1,3,7,9}

# The Euler Totient function - Properties

- So, the number of elements in reduced set of residues is called the Euler Totient Function ø(n)
- Properties:
  - If p is prime then ø(p) = p -1.
  - The function ø is multiplicative i.e. if gcd(m,n)=1, then ø(mn) = ø(m). ø(n).
  - If $n = p_1^{e1}p_2^{e2}p_3^{e3}\ldots\ldots p_k^{ek}$ is the prime factorization of n, then,

$$\text{ø}(n) = n(1-1/p_1)(1-1/p_2)(1-1/p_3)\ldots..(1-1/p_k)$$

# Euler Totient Illustration

- ø(1), ø(2), ø(3), ø(4), ø(6),ø(7), ø(14), ø(23) ø(15)
  - ø(1)= 0 - given by p = p-1
  - ø(2)=|{1}| - given by p = p-1
  - ø(3)=|{1,2}| - given by p = p-1
  - ø(4)=|{1,3}| - 4 is not a prime
  - ø(6)=|{1,5}| - 6 is not a prime
    - ø(6) = ø(3)*ø(2) = 2*1 = 2
  - ø(7)=|{ 1, 2, 3, 4, 5, 6}| - given by p = p-1
  - ø(14) = |{1,3,5,9,11,13}| - 14 is not a prime
    - ø(14) = ø(7)*ø(2) = 6*1 = 6
  - ø(23) = |{1,2,3,……22}| - 23 is prime
  - ø(15) = ?
    - 4 * 2 = 8

# Table 2.6 - Some Values of Euler's Totient Function *ø(n)*

| $n$ | $\phi(n)$ |
|---|---|
| 1 | 1 |
| 2 | 1 |
| 3 | 2 |
| 4 | 2 |
| 5 | 4 |
| 6 | 2 |
| 7 | 6 |
| 8 | 4 |
| 9 | 6 |
| 10 | 4 |

| $n$ | $\phi(n)$ |
|---|---|
| 11 | 10 |
| 12 | 4 |
| 13 | 12 |
| 14 | 6 |
| 15 | 8 |
| 16 | 8 |
| 17 | 16 |
| 18 | 6 |
| 19 | 18 |
| 20 | 8 |

| $n$ | $\phi(n)$ |
|---|---|
| 21 | 12 |
| 22 | 10 |
| 23 | 22 |
| 24 | 8 |
| 25 | 20 |
| 26 | 12 |
| 27 | 18 |
| 28 | 12 |
| 29 | 28 |
| 30 | 8 |



(This table can be found on page 48 in the textbook)

# Euler Totient Illustration

For a prime number p, $\phi(p^k) = p^k - p^{k-1}$

$$\phi(2^5) = 2^5 - 2^{5-1} = 32 - 16 = 16$$

# Euler's theorem

- Let n ≥ 2 be an integer then if $a \in Z^*_n$, then $a^{\phi(n)} \equiv 1 \pmod{n}$ (a and n are relatively prime)
- e.g.
  - $a=3; n=10; \phi(10)=4;$

    hence $3^4 = 81 \equiv 1 \bmod 10$
  - $a=2; n=11; \phi(11)=10;$

    hence $2^{10} = 1024 = 1 \bmod 11$
- If n is a product of distinct primes,
  - and if $r \equiv s \pmod{\phi(n)}$, then $a^r \equiv a^s \pmod{n}$
  - i.e. when working with modulo such as n, exponents can be reduced modulo ø(n)

# Fermat's Little theorem

- Let p be prime
  - If gcd(a, p) = 1 then
    - $a^{p-1} \equiv 1 \pmod{p}$
  - if $r \equiv s \pmod{p-1}$, then $a^r \equiv a^s \pmod{p}$ for all integers a.
  - i.e. when working with modulo a prime p, exponents can be reduced modulo p -1.
  - also $a^p \equiv a \pmod{p}$ for all integers a.
- useful in public key and primality testing

# Example

Find $3^{31} \bmod 7$.

[Solution: $3^{31} \equiv 3 \bmod 7$]

By Fermat's Little Theorem, $3^6 \equiv 1 \bmod 7$. Thus, $3^{31} \equiv 3^1 \equiv 3 \bmod 7$.

Find $2^{35} \bmod 7$.

[Solution: $2^{35} \equiv 4 \bmod 7$]

By Fermat's Little Theorem, $2^6 \equiv 1 \bmod 7$. Thus, $2^{35} \equiv 2^5 \equiv 32 \equiv 4 \bmod 7$.

# Testing for Primality

- For many cryptographic algorithms, it is necessary to select one or more very large prime numbers at random
- Thus, we are faced with the task of determining whether a given large number is prime
- However, the algorithm can yield a number that is almost certainly a prime.

# Miller-Rabin Algorithm

- This is typically used to test a large number for primality.
- Before explaining the algorithm, we need some background.
- First, any positive odd integer $n$ >= 3 can be expressed as

$$n - 1 = 2^k q \qquad \text{with } k > 0, q \text{ odd}$$

- To see this, note that $n$ - 1 is an even integer. Then, divide ($n$ - 1) by 2 until the result is an odd number $q$, for a total of $k$ divisions
- If $n$ is expressed as a binary number, then the result is achieved by shifting the number to the right until the rightmost digit is a 1, for a total of $k$ shifts.

# Miller-Rabin Algorithm…

- ***TWO PROPERTIES OF PRIME NUMBERS***
- The **first property** is stated as follows: If $p$ is prime and $a$ is a positive integer less than $p$, then $a^2 \bmod p = 1$ if and only if either $a \bmod p = 1$ or $a \bmod p = -1 \bmod p = p - 1$.
- By the rules of modular arithmetic
- $(a \bmod p)\ (a \bmod p) = a^2 \bmod p$. Thus, if either $a \bmod p = 1$ or $a \bmod p = -1$, then $a^2 \bmod p = 1$. Conversely, if $a^2 \bmod p = 1$, then $(a \bmod p)^2 = 1$, which is true.
- Thus, if either $a \bmod p = 1$ or $a \bmod p = -1$, then $a^2 \bmod p = 1$. Conversely, if $a^2 \bmod p = 1$, then $(a \bmod p)^2 = 1$, which is true only for $a \bmod p = 1$ or $a \bmod p = -1$.

# Miller-Rabin Algorithm…

- The **second property** is stated as follows: Let $p$ be a prime number greater than 2.
- We can then write $p - 1 = 2^k q$ with $k > 0$, $q$ odd.
- Let $a$ be any integer in the range $1 < a < p - 1$. Then one of the two following conditions is true.

1. $a^q$ is congruent to 1 modulo $p$. That is, $a^q \bmod p = 1$, or equivalently, $a^q \equiv 1 (\bmod p)$.
2. One of the numbers $a^q, a^{2q}, a^{4q}, \ldots, a^{2^{k-1}q}$ is congruent to $-1$ modulo $p$. That is, there is some number $j$ in the range $(1 \leq j \leq k)$ such that $a^{2^{j-1}q} \bmod p = -1 \bmod p = p - 1$ or equivalently, $a^{2^{j-1}q} \equiv -1 (\bmod p)$.

# Miller-Rabin Algorithm

- Typically used to test a large number for primality
- Algorithm is:

TEST ($n$)

1. Find integers $k$, $q$, with $k > 0$, $q$ odd, so that $(n-1)=2^k q$ ;
2. Select a random integer $a$, $1 < a < n-1$ ;
3. **if** $a^q \bmod n = 1$ **then** return ("inconclusive") ;
4. **for** $j = 0$ **to** $k-1$ **do**
5. **if** $(a^{2jq} \bmod n = n-1)$ **then** return ("inconclusive") ;
6. return ("composite") ;

# Discussion

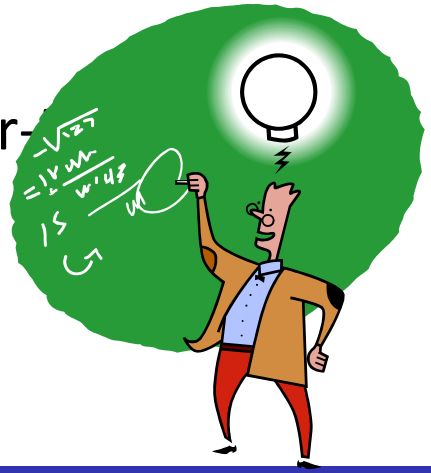
- Let us apply the test to the prime number $n = 29$.
- We have $(n - 1) = 28 = 2^2(7) = 2^k q$.
- First, let us try $a = 10$. We compute $10^7 \bmod 29 = 17$, which is neither 1 nor 28, so we continue the test.
- The next calculation finds that $(10^7)^2 \bmod 29 = 28$, and the test returns inconclusive (i.e., 29 may be prime).
- Let's try again with $a = 2$. We have the following calculations: $2^7 \bmod 29 = 12$; $2^{14} \bmod 29 = 28$; and the test again returns inconclusive.
- If we perform the test for all integers $a$ in the range 1 through 28, we get the same inconclusive result, which is compatible with $n$ being a prime number.

# Discussion…

- Now let us apply the test to the composite number $n = 13 * 17 = 221$.
- Then $(n - 1) = 220 = 2^2(55) = 2^k q$. Let us try $a = 5$. Then we have $5^{55} \bmod 221 = 112$, which is neither 1 nor $220(5^{55})^2 \bmod 221 = 168$.
- Because we have used all values of $j$ (i.e., $j = 0$ and $j = 1$) in line 4 of the TEST algorithm, the test returns composite, indicating that 221 is definitely a composite number.
- But suppose we had selected $a = 21$.
- Then we have $21^{55} \bmod 221 = 200$; $(21^{55})^2 \bmod 221 = 220$; and the test returns inconclusive, indicating that 221 may be prime.
- In fact, of the 218 integers from 2 through 219, four of these will return an inconclusive result, namely 21, 47, 174, and 200.

# Deterministic Primality Algorithm

- Prior to 2002 there was no known method of efficiently proving the primality of very large numbers
- All of the algorithms in use produced a probabilistic result
- In 2002 Agrawal, Kayal, and Saxena developed an algorithm that efficiently determines whether a given large number is prime
  - Known as the AKS algorithm
  - Does not appear to be as efficient as the Miller-[illegible] algorithm



# Chinese Remainder Theorem (CRT)

- Believed to have been discovered by the Chinese mathematician Sun-Tsu in around 100 A.D.
- One of the most useful results of number theory
- Says it is possible to reconstruct integers in a certain range from their residues modulo a set of pairwise relatively prime moduli
- Can be stated in several ways

Provides a way to manipulate (potentially very large) numbers mod *M* in terms of tuples of smaller numbers

- This can be useful when *M* is 150 digits or more
- However, it is necessary to know beforehand the factorization of *M*

# Chinese Remainder Theorem (CRT)

*Chinese Remainder Theorem:* If $m_1, m_2, .., m_k$ are pairwise relatively prime positive integers, and if $a_1, a_2, .., a_k$ are any integers, then the simultaneous congruences

$$x \equiv a_1 \pmod{m_1}, \quad x \equiv a_2 \pmod{m_2}, \quad \ldots, \quad x \equiv a_k \pmod{m_k}$$

have a solution, and the solution is unique modulo $m$, where $m = m_1 m_2 \cdots m_k$.

# Chinese Remainder Theorem (CRT)

**Given:**

$X = 3 \pmod 5$, $X = 5 \pmod 7$

**Concept:**

**Chinese Remainder Theorem:**

If $m_1, m_2, .., m_k$ are pairwise relatively prime positive integers, and if $a_1, a_2, .., a_k$ are any integers, then

The simultaneous congruences

$x \equiv a_1 \pmod{m_1}$,

$x \equiv a_2 \pmod{m_2}$

$x \equiv a_k \pmod{m_k}$

have a solution, and the solution is unique modulo M, where

$M = m_1 m_2 \cdots m_k$ .

Now, the solution x is given by

$X = M_1 X_1 a_1 + M_2 X_2 a_2 + \ldots\ldots\ldots + M_k X_k a_k$

# Chinese Remainder Theorem (CRT)

Where,

$M_i = \frac{M}{m_i}$, I = 1, 2, 3, ....K

and

$M_i X_i \equiv 1 \bmod(m_i)$

**Modulo or modulus or mod:** It is the remainder after dividing one number by another.

# Chinese Remainder Theorem (CRT)

**Calculation:**

We have given,

$m_1 = 5$ and $m_2 = 7$ which are relatively co-prime.

Also, $a_1 = 3$ and $a_2 = 5$, which are integer.

Hence the condition of the Chinese Remainder Theorem satisfied.

SO, according to the theorem, there will be the unique solution of x for modulo

$M = 5 \times 7 = 35$

Now, using the relation,

$$M_i = \frac{M}{m_i}$$

we will get

$M_1 = 7$ and $M_2 = 5$

# Chinese Remainder Theorem (CRT)

We now seek a multiplicative inverse for each $m_i$ modulo $n_i$.

Hence, we need to find inverse for 7 modulo 5
And the answer for this is 3. That is our X1=3

Hence, we need to find inverse for 5 modulo 7
And the answer for this is 5. That is our X2=3

# Chinese Remainder Theorem (CRT)

Hence the unique solution of x will be

$X = M_1X_1a_1 + M_2X_2a_2$

$\Rightarrow X = 7 \times 3 \times 3 + 5 \times 5 \times 3 = 138$

$\Rightarrow X \equiv 138 \bmod(35)$

$\Rightarrow X \equiv 33 \bmod(35)$

# Chinese Remainder Theorem (CRT)

**Example 5.** Use the Chinese Remainder Theorem to find an $x$ such that

$$x \equiv 2 \pmod 5$$
$$x \equiv 3 \pmod 7$$
$$x \equiv 10 \pmod{11}$$

**Solution.** Set $N = 5 \times 7 \times 11 = 385$. Following the notation of the theorem, we have $m_1 = N/5 = 77$, $m_2 = N/7 = 55$, and $m_3 = N/11 = 35$.
We now seek a multiplicative inverse for each $m_i$ modulo $n_i$. First: $m_1 \equiv 77 \equiv 2 \pmod 5$, and hence an inverse to $m_1$ mod $n_1$ is $y_1 = 3$.
Second: $m_2 \equiv 55 \equiv 6 \pmod 7$, and hence an inverse to $m_2$ mod $n_2$ is $y_2 = 6$.
Third: $m_3 \equiv 35 \equiv 2 \pmod{11}$, and hence an inverse to $m_3$ mod $n_3$ is $y_3 = 6$.
Therefore, the theorem states that a solution takes the form:

$$x = y_1 b_1 m_1 + y_2 b_2 m_2 + y_3 b_3 m_3 = 3 \times 2 \times 77 + 6 \times 3 \times 55 + 6 \times 10 \times 35 = 3552.$$

# Discrete Logarithms

- Consider the equation $y = g^x \bmod p$
- Given $g$, $x$, and $p$, it is a straightforward matter to calculate $y$.
- At the worst, we must perform $x$ repeated multiplications, and algorithms exist for achieving greater efficiency.
- However, given $y$, $g$, and $p$, it is, in general, very difficult to calculate $x$ (take the discrete logarithm).

# Tables of Discrete Logarithms, Modulo 19

**Table 8.4 Tables of Discrete Logarithms, Modulo 19**

**(a) Discrete logarithms to the base 2, modulo 19**

| $a$ | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | 11 | 12 | 13 | 14 | 15 | 16 | 17 | 18 |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| $\log_{2,19}(a)$ | 18 | 1 | 13 | 2 | 16 | 14 | 6 | 3 | 8 | 17 | 12 | 15 | 5 | 7 | 11 | 4 | 10 | 9 |

**(b) Discrete logarithms to the base 3, modulo 19**

| $a$ | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | 11 | 12 | 13 | 14 | 15 | 16 | 17 | 18 |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| $\log_{3,19}(a)$ | 18 | 7 | 1 | 14 | 4 | 8 | 6 | 3 | 2 | 11 | 12 | 15 | 17 | 13 | 5 | 10 | 16 | 9 |

**(c) Discrete logarithms to the base 10, modulo 19**

| $a$ | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | 11 | 12 | 13 | 14 | 15 | 16 | 17 | 18 |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| $\log_{10,19}(a)$ | 18 | 17 | 5 | 16 | 2 | 4 | 12 | 15 | 10 | 1 | 6 | 3 | 13 | 11 | 7 | 14 | 8 | 9 |

**(d) Discrete logarithms to the base 13, modulo 19**

| $a$ | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | 11 | 12 | 13 | 14 | 15 | 16 | 17 | 18 |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| $\log_{13,19}(a)$ | 18 | 11 | 17 | 4 | 14 | 10 | 12 | 15 | 16 | 7 | 6 | 3 | 1 | 5 | 13 | 8 | 2 | 9 |

**(e) Discrete logarithms to the base 14, modulo 19**

| $a$ | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | 11 | 12 | 13 | 14 | 15 | 16 | 17 | 18 |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| $\log_{14,19}(a)$ | 18 | 13 | 7 | 8 | 10 | 2 | 6 | 3 | 14 | 5 | 12 | 15 | 11 | 1 | 17 | 16 | 4 | 9 |

**(f) Discrete logarithms to the base 15, modulo 19**

| $a$ | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | 11 | 12 | 13 | 14 | 15 | 16 | 17 | 18 |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| $\log_{15,19}(a)$ | 18 | 5 | 11 | 10 | 8 | 16 | 12 | 15 | 4 | 13 | 6 | 3 | 7 | 17 | 1 | 2 | 14 | 9 |

# Abstract Algebra

- will now introduce finite fields
- of increasing importance in cryptography
  - AES, Elliptic Curve, IDEA, Public Key
- concern with operations on "numbers" where
  - what *constitutes* a "number" and the *type* of operations varies considerably
- start with concepts of groups, rings, fields from abstract algebra

# Group

- def: A group (G, *) consists of a set G with a binary operation * on G satisfying the following three axioms:
  - the group operation is associative i.e. a*(b*c) = (a*b)*c for all a,b,c $\in$ G.
  - there is an element 1 $\in$ G, called the identity element, such that a * 1 = 1 * a = a for all a $\in$ G
  - for each a $\in$ G there exists an element $a^{-1} \in$ G, called the inverse of a such that a * $a^{-1}$= $a^{-1}$ *a=1
- for a group G, if a * b = b * a for all a, b $\in$ G, then the group G is abelian or commutative.
- The set of integers (positive, negative, and 0) under addition is an abelian group.
- The set of nonzero real numbers under multiplication is an abelian group.

# Ring

- a set of “numbers”
- with two operations (addition and multiplication) denoted as (R, +, X) and
  - which forms an abelian group with addition operation (identity 0)
  - multiplication operation
    - has closure
    - is associative i.e. a x (b x c) = (a x b) x c for all a,b,c $\in$ R
    - distributive over addition i.e. a x (b+c) = a x b + a x c
- i.e. a ring is a set in which we can do addition, subtraction and multiplication without leaving the set.
- e.g. the set of integers Z with + supported is a ring
- With respect to addition and multiplication, the set of all n-square matrices over the real numbers is a ring.

# Ring (contd)

- if multiplication operation is commutative, it forms a commutative ring
  - e.g. the set $Z_n$ with + and x performed modulo n is a commutative ring.
  - the set $Z_{even}$ with + and x is a commutative ring

# 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 $b = 0$. |

- if multiplication operation has an identity and no zero divisors, it forms an integral domain
- e.g. the set of integers, positive, negative and 0 under + and x is an integral domain.

# Invertible element and Field

- An element a of a ring R is called a unit or an invertible element
  - if there is an element $b \in R$ such that $a \times b = 1$.
- A field is a set of numbers with two operations which form
  - an abelian group for addition
  - an abelian group for multiplication (ignoring 0)
  - ring

# Field (contd)

- def: A field is a commutative ring in which all the non-zero elements have multiplicative inverses.
- $Z_n$ is a field if n is a prime number.
- These have hierarchy with more axioms/laws
  - group -> ring -> field

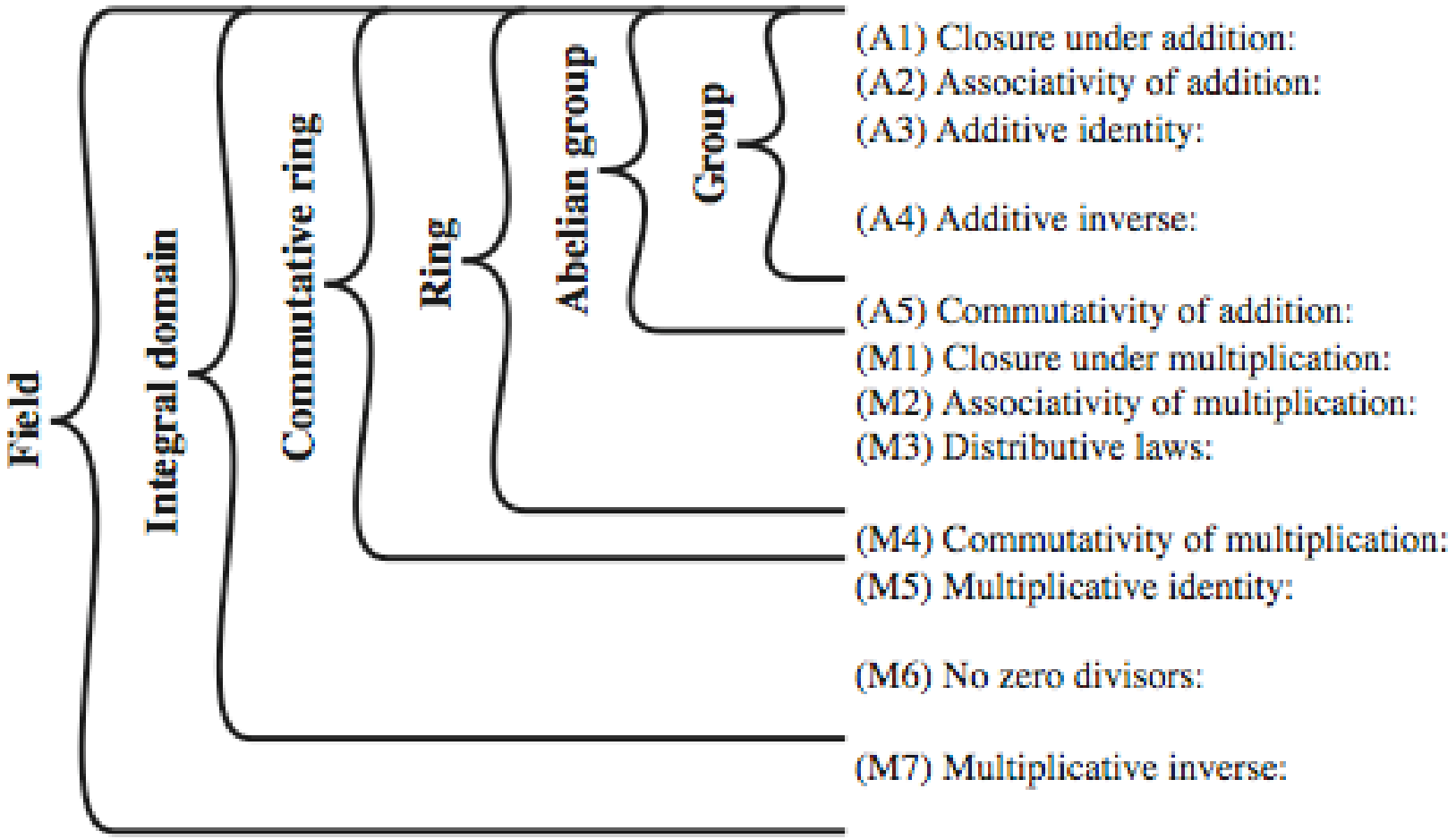
# Galois Fields

- Infinite fields are of not much interest. But,
- finite fields play a key role in cryptography
- it can be shown that the number of elements in a finite field
  - i.e. the order of a finite filed must be a power of a prime $p^n$, $n \geq 1$
  - the finite field of the order of $p^n$ are known as Galois fields
- denoted $GF(p^n)$
- in particular often use the fields
  - GF(p)
  - $GF(2^n)$

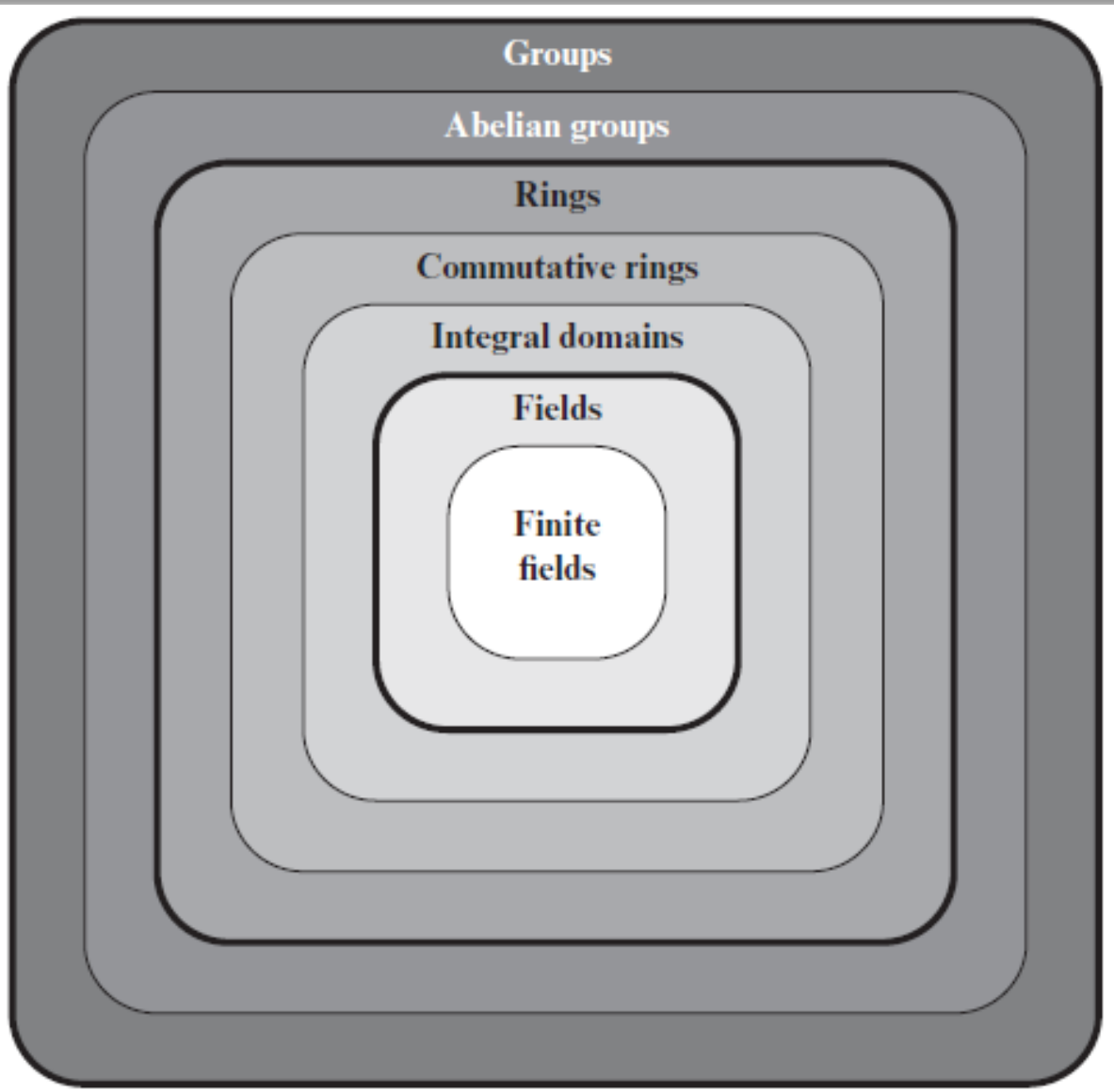
# Galois Fields GF(p)

- GF(p) is the set of integers $Z_p$ ={0,1, … , p-1} with arithmetic operations modulo prime p
- these form a finite field - since each element has multiplicative inverse
- hence arithmetic is “well-behaved” and
  - can do addition, subtraction, multiplication, and division without leaving the field GF(p)

# Group, Ring, Field



# Group, Ring, Field…



# Polynomial Arithmetic with Coefficients in $Z_p$

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

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

Figures 5.5a through 5.5c show the manual calculations. We comment on division subsequently.

# Polynomial Arithmetic with Coefficients in $Z_p$

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

(a) Addition

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

(b) Subtraction

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

(c) Multiplication

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

(d) Division

# Thank You !!!