Number Theory and Cryptography

ANISHA JOSEPH

Divisibility

Given two integers a and d with d non-zero, we say that d **divides** a (written **d | a**) if there is an integer c with a = cd.

If no such integer exists, so d **does not divide** a, we write **d ∤ a.** If d divides a, we say that d is a divisor of a.

Eg: 5 | 30 since 30 = 5 · 6

3 | 102 since 102 = 3 · 34

6 ∤ 23 (since 23/6 is not an integer)

4 ∤ −3 (since 4/(−3) is not an integer)

−7 | 35, 8 | 8, 3 | 0, −2 | −10, and 1 | 4.

Divisibility

Preposition: Assume that a, b, and c are integers. If $a \mid b$ and $b \mid c$, then $a \mid c$.

Preposition: Assume that a, b, d, x, and y are integers. If $d \mid a$ and $d \mid b$ then $d \mid ax + by$.

Corollary: Assume that a, b, and d are integers. If $d \mid a$ and $d \mid b$, then $d \mid a + b$ and $d \mid a - b$.

The Division Algorithm

Let *a* and *b* be integers with *b > 0*. Then *there exist unique integers q* (the quotient) and *r (the remainder)* so that

$$\mathbf{a = bq + r}$$

with $0 \leq r < b$.

Eg: Let a = 27, b = 7. Then $27 = 7 \cdot 3 + 6$, so q = 3 and r = 6.

(b) Let a = −27, b = 7. Then $-27 = 7 \cdot (-4) + 1$, so q = −4 and r = 1.

(c) Let a = 24, b = 8. Then $24 = 8 \cdot 3$, so q = 3 and r = 0.

(d) Let a = 0 and b = 5. Then $0 = 5 \cdot 0 + 0$, so q = 0 and r = 0.

The Euclidean Algorithm

Let a and b be non-negative integers and assume that b ≠ 0. Do the following computation:

$$
\begin{aligned}
a &= q_1 b \ + r_1, \ \ with\ 0 \le r_1 < b \\
b &= q_2 r_1 + r_2, \ \ with\ 0 \le r_2 < r_1 \\
r_1 &= q_3 r_2 + r_3, \ \ with\ 0 \le r_3 < r_2 \\
&\vdots \\
r_{n-3} &= q_{n-1} r_{n-2} + r_{n-1}, \ \ with\ 0 \le r_{n-1} < r_{n-2} \\
r_{n-2} &= q_n r_{n-1} + 0.
\end{aligned}
$$

The last non-zero remainder, namely rn−1, equals gcd(a, b).

The Euclidean Algorithm

1. **Compute gcd(123, 456).**

$456 = 3 \cdot 123 + 87$

$123 = 1 \cdot 87 + 36$

$87 = 2 \cdot 36 + 15$

$36 = 2 \cdot 15 + 6$

$15 = 2 \cdot 6 + 3$

$6 = 2 \cdot 3 + 0.$

2. **Compute gcd(119, 259)**

Extended Euclidean Algorithm

- The Euclidean Algorithm yields an amazing and very useful fact gcd(a, b) can be expressed as a linear combination of a and b.
- That is, there exist integers s and t such that gcd(a, b) = as+ bt.

2.11.3 Computer Explorations

1. Define a function on positive integers by

$$f(n) = \begin{cases} n/2 \text{ if } n \text{ is even} \\ 3n+1 \text{ if } n \text{ is odd.} \end{cases}$$

For example, $f(5) = 16$ and $f(6) = 3$. If we start with a positive integer m, we can form the sequence $m_1 = f(m)$, $m_2 = f(m_1)$, $m_3 = f(m_2)$, etc. The *Collatz Conjecture* predicts that we eventually get $m_k = 1$ for some k. For example, if we start with $m = 7$, we get $m_1 = 22$, $m_2 = 11$, $m_3 = 34$, $m_4 = 17$, $m_5 = 52$, $m_6 = 26$, $m_7 = 13$, $m_8 = 40$, $m_9 = 20$, $m_{10} = 10$, $m_{11} = 5$, $m_{12} = 16$, $m_{13} = 8$, $m_{14} = 4$, $m_{15} = 2$, $m_{16} = 1$.
(a) Show that the Collatz Conjecture is true for all $m \leq 60$. Which starting value of m required the most steps?
(b) Suppose you change $3n+1$ to $n+1$ in the definition of $f(n)$. What happens? Can you prove this?
(c) Suppose you change $3n+1$ to $5n+1$ in the definition of $f(n)$. Try a few examples and see what happens. Do you see a different behavior for starting values $m = 5$, $m = 6$, and $m = 7$?

3. Find 20 examples of numbers that are sixth powers. What is true about the remainders when these sixth powers are divided by 7? Can you make a conjecture and then prove it?

4. Write a program that generates 10000 "random" pairs (a, b) of integers, and then use the Euclidean Algorithm (or your software gcd routine) to decide whether $\gcd(a, b) = 1$. If m is the number of pairs that are relatively prime, calculate

$$\frac{m}{10000},$$

which is the fraction of these pairs that are relatively prime. Follow the same procedure for 10^5 pairs and then 10^6 pairs. Can you make a guess as to what number this ratio approaches? (*Hint:* It is an integer divided by π^2.)

Congruences

Two integers a and b are **congruent mod m** (written $a \equiv b \pmod{m}$) **if a−b is a multiple of m.** The integer m is called the modulus of the congruence and is assumed to be positive.

Eg:

$7 \equiv 1 \pmod{2}$, $14 \equiv 0 \pmod{2}$, $19 \equiv 7 \pmod{6}$,

$-8 \equiv 12 \pmod{5}$, $4 \equiv 4 \pmod{11}$, $6 \equiv 16 \pmod{5}$,

$34 \equiv 12 \pmod{11}$, $7 \equiv -2 \pmod{3}$, $-11 \equiv 3 \pmod{7}$

Congruences

- n is even if and only if $n \equiv 0 \pmod 2$ and n is odd if and only if $n \equiv 1 \pmod 2$.
- $2347 \equiv 7 \pmod{10}$, $65931 \equiv 1 \pmod{10}$, $2347 \equiv 47 \pmod{100}$, and $65931 \equiv 31 \pmod{100}$. Generally, two positive integers are congruent mod 10 if their last digits are the same, and they are congruent mod 100 if the last two digits of one are the same as the last two digits of the other.

Congruences

- $4 \equiv 4 \pmod 8$, $12 \equiv 4 \pmod 8$, $20 \equiv 4 \pmod 8$, and $28 \equiv 4 \pmod 8$ and so on.
- $11 \equiv 1 \pmod 5$, $12 \equiv 2 \pmod 5$ and $13 \equiv 3 \pmod 5$ and so on.

$a \equiv b \pmod m$ if and only if $a = b + km$ for some integer k

Properties of Congruences

Congruences have the following properties:

1. $a \equiv b \pmod{m}$ if $m \mid (a - b)$.
2. $a \equiv b \pmod{m}$ implies $b \equiv a \pmod{m}$.
3. $a \equiv b \pmod{m}$ and $b \equiv c \pmod{m}$ imply $a \equiv c \pmod{m}$.

Congruence classes mod m or Residue classes

One set consists of all the integers that are congruent to 0 mod m, another of the integers congruent to 1 mod m, then the integers congruent to 2 mod m until we get to the set which is made of the integers that are m− 1 mod m. These m sets are called **congruence classes mod m.**

Congruence classes mod m or Residue classes

For example, if m = 5, the five congruence classes are,

All integers congruent to 0 mod 5: {· · · – 10,–5, 0, 5, 10, 15, · · · }

All integers congruent to 1 mod 5: {· · · – 9,–4, 1, 6, 11, 16, · · · }

All integers congruent to 2 mod 5: {· · · – 8,–3, 2, 7, 12, 17, · · · }

All integers congruent to 3 mod 5: {· · · – 7,–2, 3, 8, 13, 18, · · · }

All integers congruent to 4 mod 5: {· · · – 6,–1, 4, 9, 14, 19, · · · }

Congruence classes mod m or Residue classes

These numbers are in the same congruence class mod m. For example, −3 and 17 are in the same congruence class mod 5 and $-3 \equiv 17 \pmod 5$.

Complete system of residues modulo m

Let m be a positive integer. A set of integers $a_1, a_2, \ldots, a_m$ is called a complete system of residues modulo m, **if the set contains exactly one element from each residue class modulo m.**

Let m = 5. Then {−10, 11, 2, -7, 9} is a complete system of residues modulo 5, since $-10 \in [0]$, $11 \in [1]$, $2 \in [2]$, $-7 \in [3]$ and $9 \in [4]$. Of course, it can be easily verified that {-5,1,−3, -2, 4} is another complete system of residues modulo 5.

Reduced Residue systems

Let $[a]_m$ be a residue class modulo m. We say that $[a]_m$ is relatively prime to m if each element in $[a]_m$ is relatively prime to m.

Let n = 10. Then the ten residue classes, modulo 10, are as follows:

Clearly, $[1]_{10,}$, $[3]_{10}$, $[7]_{10}$, and $[9]_{10}$ are residue classes that are relatively prime to 10.

$$[0]_{10} = \{\ldots, -30, -20, -10, 0, 10, 20, 30, \ldots\}$$

$$[1]_{10} = \{\ldots, -29, -19, -9, 1, 11, 21, 31, \ldots\}$$

$$[2]_{10} = \{\ldots, -28, -18, -8, 2, 12, 22, 32, \ldots\}$$

$$[3]_{10} = \{\ldots, -27, -17, -7, 3, 13, 23, 33, \ldots\}$$

$$[4]_{10} = \{\ldots, -26, -16, -6, 4, 14, 24, 34, \ldots\}$$

$$[5]_{10} = \{\ldots, -25, -15, -5, 5, 15, 25, 35, \ldots\}$$

$$[6]_{10} = \{\ldots, -24, -14, -4, 6, 16, 26, 36, \ldots\}$$

$$[7]_{10} = \{\ldots, -23, -13, -3, 7, 17, 27, 37, \ldots\}$$

$$[8]_{10} = \{\ldots, -22, -12, -2, 8, 18, 28, 38, \ldots\}$$

$$[9]_{10} = \{\ldots, -21, -11, -1, 9, 19, 29, 39, \ldots\}.$$

Reduced Residue systems

- If a **residue class modulo m** has one element which is relatively prime to m, then every element in that residue class is relatively prime to m.
- If a residue class modulo m has one element which is relatively prime to m, then every element in that residue class is relatively prime to m.
- If m is prime, then every residue class modulo m (except $[0]_m$) is relatively prime to m.

Reduced Residue systems

- Let m be a positive integer, then **$\phi(m)$** is the number of residue classes modulo m, which is relatively prime to m.
- A set of integers $\{a_1, a_2, \ldots, a_{\phi(m)}\}$ is called a **reduced system of residues,** if the set contains exactly one element from each residue class modulo m which is relatively prime to m.

Reduced Residue systems

Example:

we know that $[1]_{10}$, $[3]_{10}$, $[7]_{10}$, and $[9]_{10}$ are residue classes that are relatively prime to 10, so by choosing −29 from $[1]_{10}$, −17 from $[3]_{10}$, 17 from $[7]_{10}$ and 39 from $[9]_{10}$, we get a reduced system of residues modulo 10: {−29,−17, 17, 39}.

Similarly, {31, 3,−23,−1} is another reduced system of residues modulo 10.

least residue modulo m

- The set of all of these least (nonnegative) residues is what we have shown as $Z_5 = \{0, 1, 2, 3, 4\}$.
- In other words, the set Z_m is the set of all **least residue modulo m.**

Operations in z_n

Example 2.16

Perform the following operations (the inputs come from $\mathbf{Z}_n$):

a. Add 7 to 14 in $\mathbf{Z}_{15}$.

b. Subtract 11 from 7 in $\mathbf{Z}_{13}$.

c. Multiply 11 by 7 in $\mathbf{Z}_{20}$.

Solution

The following shows the two steps involved in each case:

$$(14 + 7) \bmod 15 \rightarrow (21) \bmod 15 = 6$$
$$(7 - 11) \bmod 13 \rightarrow (-4) \bmod 13 = 9$$
$$(7 \times 11) \bmod 20 \rightarrow (77) \bmod 20 = 17$$

Operations in z_n

Example 2.17

Perform the following operations (the inputs come from either $\mathbf{Z}$ or $\mathbf{Z}_n$):

a. Add 17 to 27 in $\mathbf{Z}_{14}$.

b. Subtract 43 from 12 in $\mathbf{Z}_{13}$.

c. Multiply 123 by −10 in $\mathbf{Z}_{19}$.

Solution

The following shows the two steps involved in each case:

$$
\begin{aligned}
(17 + 27) \bmod 14 &\rightarrow (44) \bmod 14 = 2 \\
(12 - 43) \bmod 13 &\rightarrow (-31) \bmod 13 = 8 \\
(123 \times (-10)) \bmod 19 &\rightarrow (-1230) \bmod 19 = 5
\end{aligned}
$$

Properties

Three binary operations in the modular arithmetic can come from Z or Z_m.

First Property: $(a + b) \bmod m = [(a \bmod m) + (b \bmod m)] \bmod m$

Second Property: $(a - b) \bmod m = [(a \bmod m) - (b \bmod m)] \bmod m$

Third Property: $(a \times b) \bmod m = [(a \bmod m) \times (b \bmod m)] \bmod m$

Properties

Example 2.18

The following shows the application of the above properties:

1. $(1{,}723{,}345 + 2{,}124{,}945) \bmod 11 = (8 + 9) \bmod 11 = 6$
2. $(1{,}723{,}345 - 2{,}124{,}945) \bmod 16 = (8 - 9) \bmod 11 = 10$
3. $(1{,}723{,}345 \times 2{,}124{,}945) \bmod 16 = (8 \times 9) \bmod 11 = 6$

Properties

Exponentiation a^n (mod m) is performed by repeated multiplication, as in ordinary arithmetic.

To find $11^7 \bmod 13$, we can proceed as follows:

$$11^2 = 121 \equiv 4 \pmod{13}$$

$$11^4 = (11^2)^2 \equiv 4^2 \equiv 3 \pmod{13}$$

$$11^7 = 11 \times 11^2 \times 11^4$$

$$11^7 \equiv 11 \times 4 \times 3 \equiv 132 \equiv 2 \pmod{13}$$

Modular Exponentiation

Compute $3^{385} \pmod{479}$

Ans: 327

Modular Exponentiation

$$3^4 \equiv 9^2 \equiv 81$$

$$3^8 \equiv 81^2 \equiv 6561 \equiv 334$$

$$3^{16} \equiv 334^2 \equiv 111556 \equiv 428$$

$$3^{32} \equiv 428^2 \equiv 183184 \equiv 206$$

$$3^{64} \equiv 206^2 \equiv 284$$

$$3^{128} \equiv 284^2 \equiv 184$$

$$3^{256} \equiv 184^2 \equiv 326.$$

How does this help? Since the exponent $385 = 256 + 128 + 1$, we have

$$3^{385} \equiv 3^{256} \cdot 3^{128} \cdot 3^1 \equiv 326 \cdot 184 \cdot 3 \equiv 327.$$

Identity element

Modular Additive Identity:

As in normal arithmetic, **zero** (or any other element of the congruence class containing zero) is the identity element and exhibits the following behavior.

$$a + 0 \equiv a \pmod{n}$$

I.e 0+a = a+0 = a

Modular Multiplicative Identity:

Modular multiplication has the same identity element as ordinary multiplication and the rules are identical.

$$\square\square(a)(1)\square \equiv a \pmod{n}$$

I.e 1*a = a*1 = a

Inverses

Additive Inverse: In Z_m, two numbers a and b are additive inverses of each other if **$a + b \equiv 0 \pmod{n}$.**

Eg: The additive inverse of 4 in Z_{10} is $10 - 4 = 6$.

Note: In modular arithmetic, each integer has an additive inverse. The sum of an integer and its additive inverse is congruent to 0 modulo m.

Multiplicative Inverse

- In Z_m, two numbers a and b are multiplicative inverse of each other if **$a \times b \equiv 1 \pmod{m}$.**

  It can be denoted as **a is** b^{-1} **modulo m** and **b is** a^{-1} **modulo m.**

- For example, if the modulus is 10, then the multiplicative inverse of 3 is 7. In other words, we have $(3 \times 7) \bmod 10 = 1$.
- **Note:** In modular arithmetic, an integer may or may not have a multiplicative inverse.
- When it does, the product of the integer and it multiplicative inverse is congruent to 1 modulo m.

Multiplicative Inverse

a has a multiplicative inverse in Z_m if and only if gcd (m, a) = 1. In this case, a and m are said to be relatively prime.

1. Find the multiplicative inverse of 8 in Z_{10}.

Solution: There is no multiplicative inverse because gcd (10, 8) = 2 ≠ 1.

2. Find all multiplicative inverses in Z_{10}.

Solution: There are only three pairs: (1, 1), (3, 7) and (9, 9). The numbers 0, 2, 4, 5, 6, and 8 do not have a multiplicative inverse.

Example

Additive modulo 5

+	0	1	2	3	4
0	0	1	2	3	4
1	1	2	3	4	0
2	2	3	4	0	1
3	3	4	0	1	2
4	4	0	1	2	3

multiplication modulo 5

X	0	1	2	3	4
0	0	0	0	0	0
1	0	1	2	3	4
2	0	2	4	1	3
3	0	3	1	4	2
4	0	4	3	2	1

Find inverse using extended euclidean algorithm

Questions

Fermat's theorem

Fermat's theorem states the following: If p is prime and a is a positive integer not divisible by p, then

$$a^{p-1} \equiv 1 \pmod{p}$$

Example. Divide 23 into 7^{200}. What is the remainder? By Fermat's theorem, $7^{22} \equiv 1 \pmod{23}$. Therefore,

$$7^{200} \equiv (7^{22})^9 \cdot 7^2 \equiv 1^9 \cdot 49 \equiv 3 \pmod{23}.$$

Compute $2^{104} \pmod{101}$: Ans 16

Euler's Theorem

Let n be a positive integer. Define the **Euler-ϕ function ϕ(n)** also called as **Euler's totient function** to be the number of integers j with $1 \le j \le n$ such that gcd(j, n) = 1.

Examples.

1. $\phi(3) = 2$ since $j = 1$ and $j = 2$ have $\gcd(j, 3) = 1$.
2. $\phi(4) = 2$.
3. $\phi(12) = 4$ (the numbers are 1, 5, 7, 11).
4. $\phi(1) = 1$ (the only value of j is $j = 1$; this is the reason we have $j \le n$ rather than $j < n$ in the definition).
5. If p is prime, then $\phi(p) = p - 1$.

Euler's Theorem

$\phi(3) = 3-1=2$

Proposition 8.6. *Let m, n be positive integers. If $\gcd(m,n) = 1$ then*

$$\phi(mn) = \phi(m) \cdot \phi(n).$$

$\phi(21) = \phi(3) * \phi(7) = (3 - 1) * (7 - 1) = 2 * 6 = 12$

Proposition 8.7. *If p is a prime and $k \geq 1$, then $\phi(p^k) = p^k - p^{k-1}$.*

Example. Let's evaluate $\phi(100)$. The first formula says that

$$\phi(100) = \phi(2^2)\phi(5^2) = (2^2 - 2)(5^2 - 5) = 40.$$

Euler's Theorem

Theorem 8.9. *(Euler's Theorem) Let n be a positive integer and let b be an integer with $\gcd(b, n) = 1$. Then*

$$b^{\phi(n)} \equiv 1 \pmod{n}.$$

Remark. Notice that Euler's theorem generalizes Fermat's theorem since $\phi(p) = p - 1$ and if b is not a multiple of p, then $\gcd(b, p) = 1$.

Questions

Find the remainder when 3^{100} is divided by 7.

Find the remainder when 7^{20} is divided by 21.

Wilson's Theorem

Let p be prime, Then **(p – 1)! ≡ –1 (mod p).**

Example. Let $p = 7$. Then

$$(p-1)! = 6! = 720 \equiv -1 \pmod{7}.$$

Proof. Let's see why the example works. Rearrange the factorial as

$$6! \equiv (6)(5 \cdot 3)(4 \cdot 2)(1) \equiv (-1)(1)(1)(1) \pmod{7}.$$

Wilson's Theorem

Example. Here is another example of what happened in the proof of Wilson's theorem. Let $p = 11$. Then

$$\begin{aligned}(p-1)! = 10! &\equiv (10)(9\cdot 5)(8\cdot 7)(6\cdot 2)(4\cdot 3)(1)\\ &\equiv (10)(1)(1)(1)(1)(1) \equiv 10 \equiv -1 \pmod{11}.\end{aligned}$$

Wilson's Theorem

Corollary: Let n ≥ 2 be an integer. Then n is prime if and only if (n − 1)! ≡ −1 (mod n).

Example. Let $n = 6$. Then

$$(n-1)! = 5! = 120 \equiv 0 \pmod{6},$$

which implies that 6 is not prime.

Wilson's Theorem

Show how the numbers match up in the proof of Wilson’s theorem for p = 13.

8.5.3 Computer Explorations

1. (a) A prime p is called a *Wieferich prime* if $2^{p-1} \equiv 1 \pmod{p^2}$. There are only two such primes known. Both are less than 4000. Can you find them?
   (b) A prime p is called a *Mirimanoff prime* if $3^{p-1} \equiv 1 \pmod{p^2}$. There are two such primes known. One is small and the other is slightly larger than 1 million. Can you find them?
   (c) Can you find other examples of primes p where $r^{p-1} \equiv 1 \pmod{p^2}$ for a small prime r?
   Wieferich primes and Mirimanoff primes arose in connection with Fermat's Last Theorem.

Chinese Remainder Theorem (CRT)

The Chinese remainder theorem (CRT) is used to solve a set of congruent equations with one variable but different moduli, which are relatively prime, as shown below:

$$
\begin{aligned}
x &\equiv a_1 \pmod{m_1} \\
x &\equiv a_2 \pmod{m_2} \\
&\cdots \\
x &\equiv a_k \pmod{m_k}
\end{aligned}
$$

Chinese Remainder Theorem (CRT)

1. Find $M = m_1 \times m_2 \times \cdots \times m_k$. This is the common modulus.
2. Find $M_1 = M/m_1$, $M_2 = M/m_2$, …, $M_k = M/m_k$.
3. Find the multiplicative inverse of M_1, M_2, …, M_k using the corresponding moduli (m_1, m_2, …, m_k). Call the inverses M_1^{-1}, M_2^{-1}, …, M_k^{-1}.
4. The solution to the simultaneous equations is

$$x = (a_1 \times M_1 \times M_1^{-1} + a_2 \times M_2 \times M_2^{-1} + \cdots + a_k \times M_k \times M_k^{-1}) \bmod M$$

Chinese Remainder Theorem (CRT)

Find the solution to the simultaneous equation.

$$
\begin{aligned}
x &\equiv 2 \bmod 3 \\
x &\equiv 3 \bmod 5 \\
x &\equiv 2 \bmod 7
\end{aligned}
$$

From the previous example, we already know that the answer is $x = 23$. We follow the four steps

1. $M = 3 \times 5 \times 7 = 105$
2. $M_1 = 105 / 3 = 35, \quad M_2 = 105 / 5 = 21, \quad M_3 = 105 / 7 = 15$
3. The inverses are $M_1^{-1} = 2, M_2^{-1} = 1, M_3^{-1} = 1$
4. $x = (2 \times 35 \times 2 + 3 \times 21 \times 1 + 2 \times 15 \times 1) \bmod 105 = 23 \bmod 105$

Computer Explorations

6. (a) Solve the simultaneous congruences

$$n \equiv 0 \pmod 4, \quad n \equiv -1 \pmod 9, \quad n \equiv -2 \pmod{25},$$
$$n \equiv -3 \pmod{49}, \quad n \equiv -5 \pmod{121}$$

to find six consecutive integers that are not squarefree.
(b) Find the smallest positive integer n such that $n, n+1, n+2, n+3, n+4, n+5$ are not squarefree. The answer should be much smaller than the number from part (a).

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.

Following obeyed for addition(+):

- **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.

FIELDS

- **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.

Following obeyed for multiplication(*):

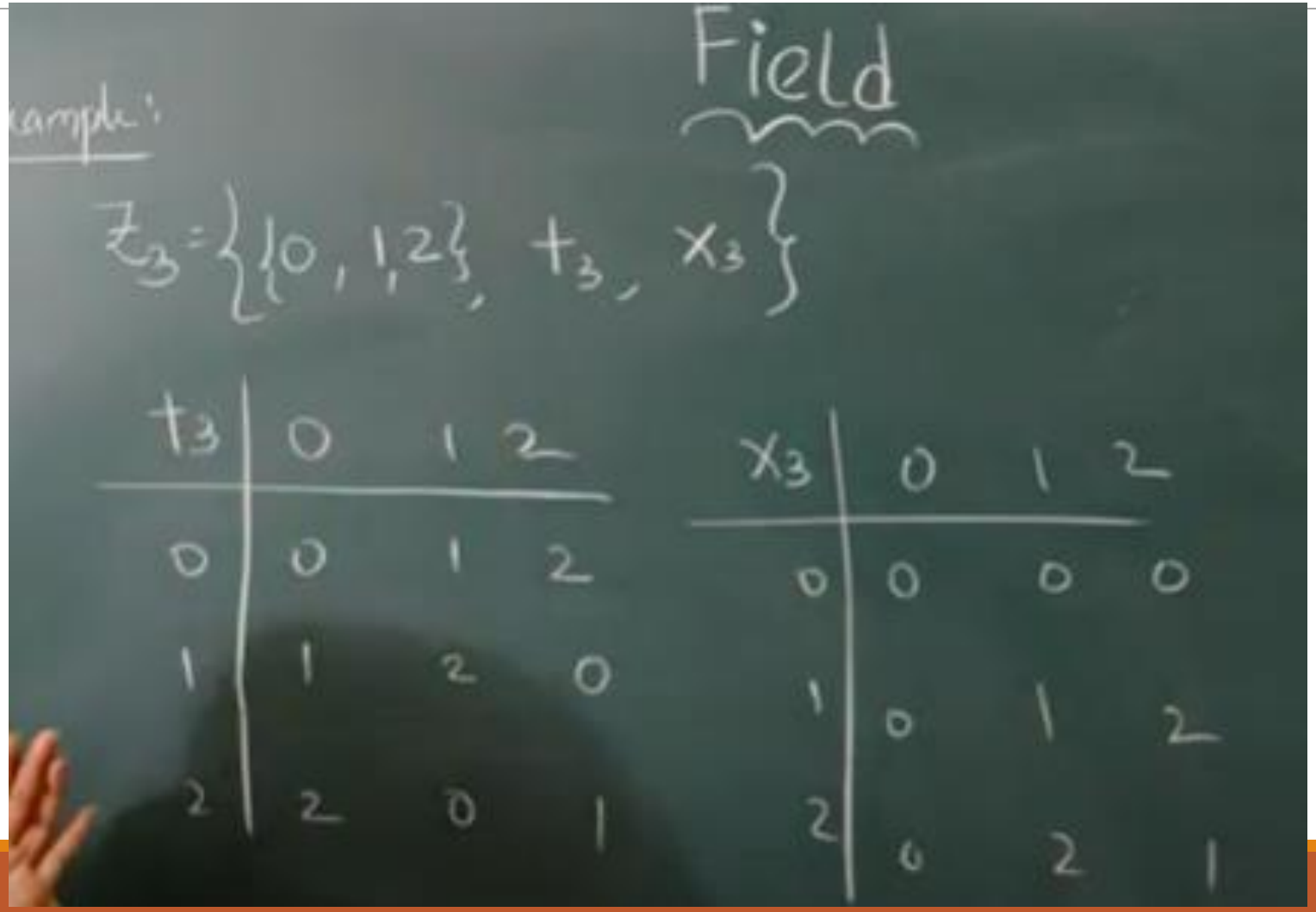
- **M1- Closure under multiplication:** If a and b belong to R, then a*b is also in R.
- **M2- Associativity of multiplication:** a*(b*c) = (a*b)*c for all a, b, c in R.
- **M3: Distributive laws:** a*(b + c) = a*b + a*c for all a, b, c in R.

  (a + b)*c = a*c + b*c for all a, b, c in R.

FIELDS

- **M4 - Commutativity of multiplication:** a*b = b*a for all a, b in R.
- **M5 - Multiplicative identity:** There is an element 1 in R such that a*1 = 1*a = a for all a in R.
- **M6 - No zero divisors:** If a, b in R and a*b = 0, then either a = 0 or b = 0.
- **M7- Multiplicative inverse:** For each a in F, except 0, there is an element a^{-1} in F such that a* a^{-1} = (a^{-1}) * a = 1.

FIELDS


Field
$Z_3 = \{0, 1, 2\}, +_3, \times_3$
$+_3$ | 0 1 2
0 | 0 1 2
1 | 1 2 0
2 | 2 0 1
$\times_3$ | 0 1 2
0 | 0 0 0
1 | 0 1 2
2 | 0 2 1

Finite Fields of Order p

For a given prime, p, we define the finite field of order p, GF(p), as the set Z_p of integers $\{0, 1, \ldots, p-1\}$ together with the arithmetic operations modulo p. Note therefore that we are using ordinary modular arithmetic to define the operations over these fields.

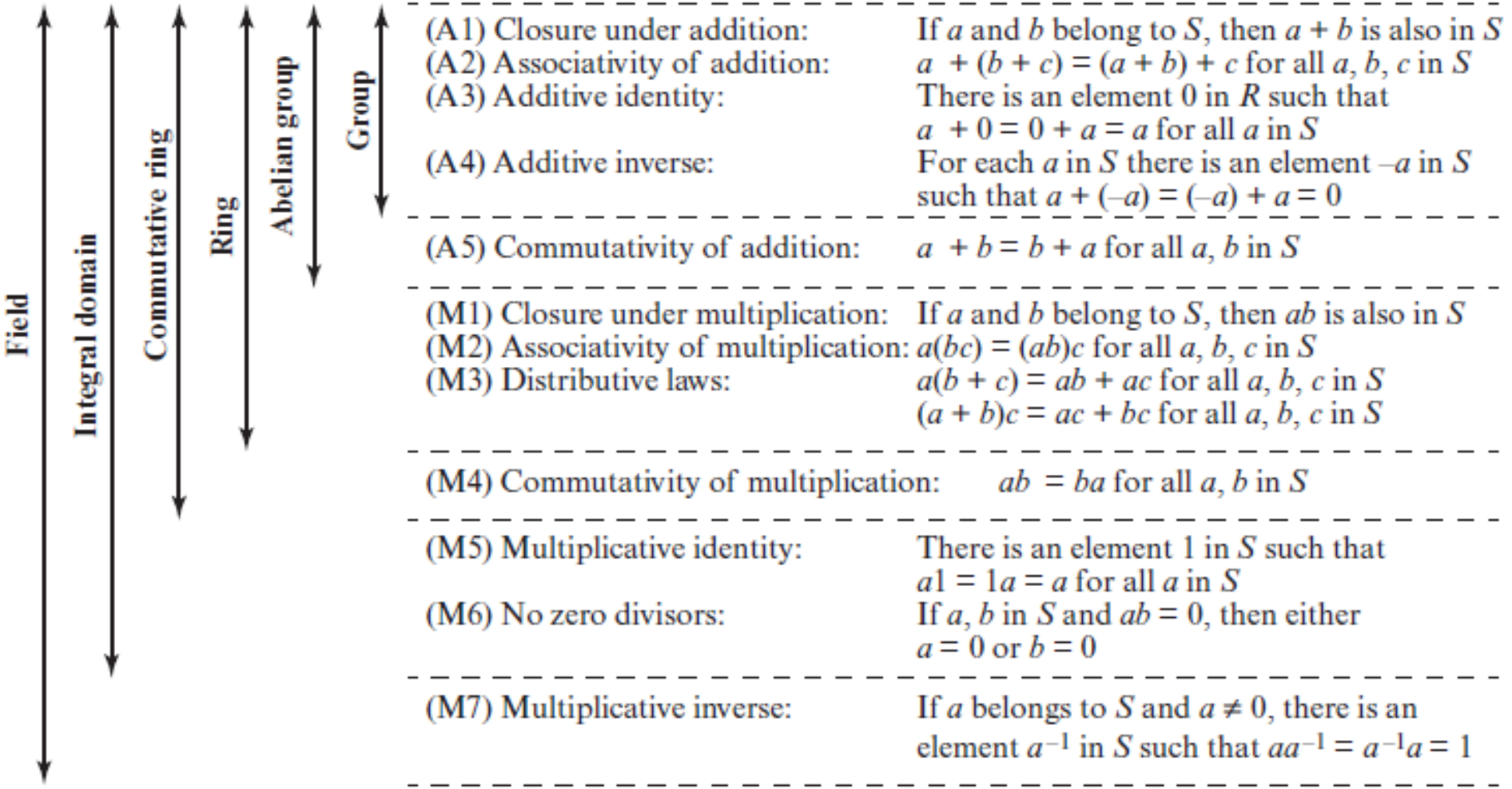


Figure 5.2 Properties of Groups, Rings, and Fields

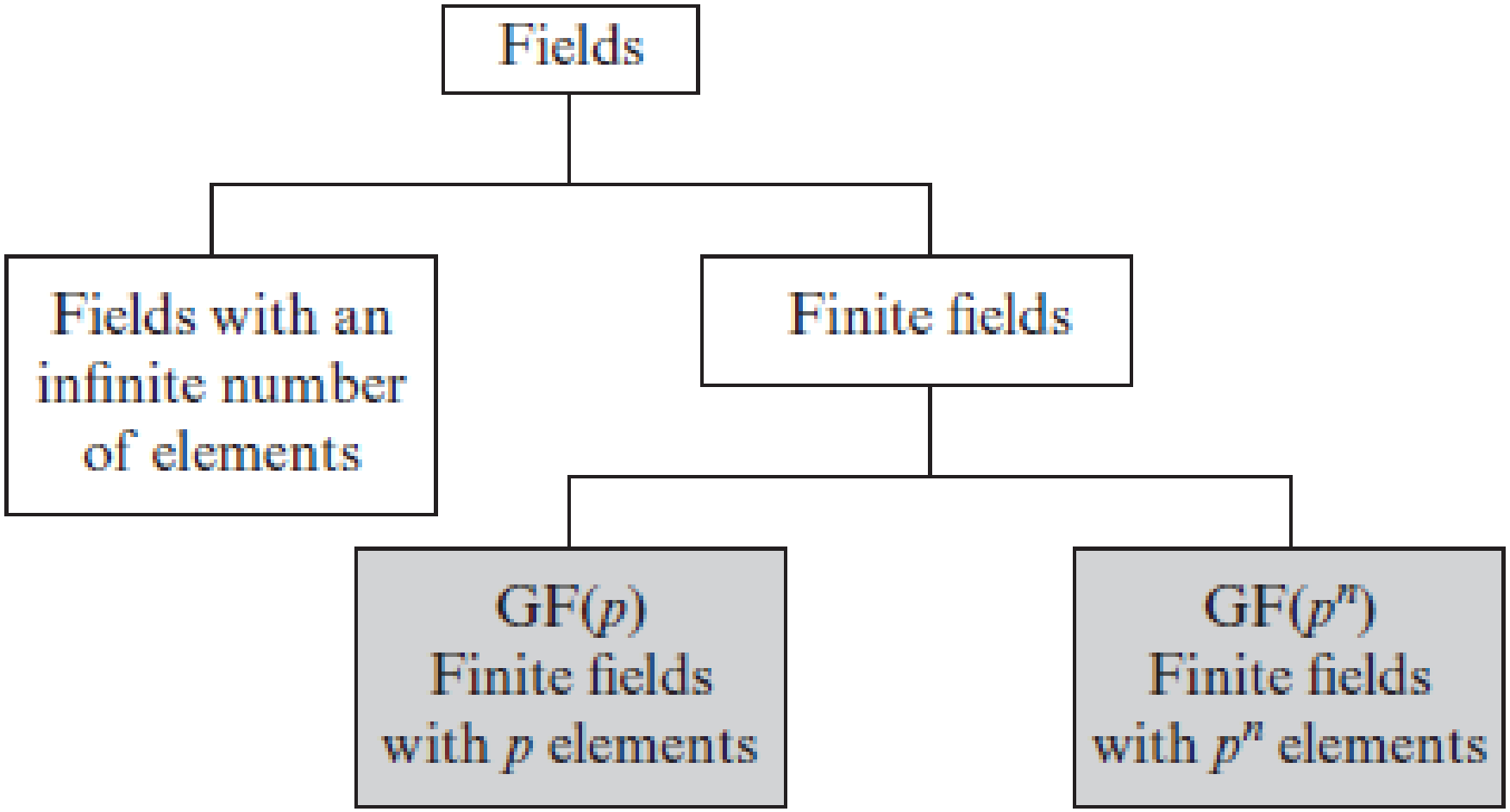


Figure 5.3 Types of Fields

FINITE FIELDS OF THE FORM GF(p)

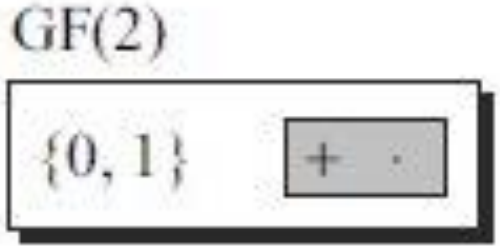
Finite Fields of Order p (GF(p)):

For a given prime, p, we define the finite field of order p, GF(p), (GF stands for Galois field), as the set Zp of integers {0, 1, ..., p - 1} together with the two arithmetic operations (addition and multiplication) modulo p.

FINITE FIELDS OF THE FORM GF(p)

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

Figure 4.6 *GF(2) field*



+	0	1
0	0	1
1	1	0

Addition

·	0	1
0	0	0
1	0	1

Multiplication

FINITE FIELDS OF THE FORM GF(p)

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

Figure 4.7 *GF(5) field*

GF(5)

{0, 1, 2, 3, 4} + ×

+	0	1	2	3	4
0	0	1	2	3	4
1	1	2	3	4	0
2	2	3	4	0	1
3	3	4	0	1	2
4	4	0	1	2	3

Addition

×	0	1	2	3	4
0	0	0	0	0	0
1	0	1	2	3	4
2	0	2	4	1	3
3	0	3	1	4	2
4	0	4	3	2	1

Multiplication

Additive inverse

a	0	1	2	3	4
$-a$	0	4	3	2	1

a	0	1	2	3	4
a^{-1}	—	1	3	2	4

Multiplicative inverse

GF(P^n) Fields

- GF(P^n) Fields In addition to GF(p) fields, we are also interested in GF(P^n) fields in cryptography.
- However, when we work with computers, the positive integers are stored in the computer as n-bit words in which n is usually 8, 16, 32, 64, and so on.
- Virtually all **encryption algorithms, both symmetric and asymmetric, involve arithmetic operations on integers**. If one of the operations that is used in the algorithm is division, then we need to work in arithmetic defined over a field.

GF(P^n) Fields

2. We can work in GF(2^n) and uses a set of 2^n elements. The elements in this set are n-bit words. For example, if $n = 3$, the set is

$$\{000, 001, 010, 011, 100, 101, 110, 111\}$$

Example 4.14

Let us define a GF(2^2) field in which the set has four 2-bit words: {00, 01, 10, 11}. We can redefine addition and multiplication for this field in such a way that all properties of these operations are satisfied, as shown in Figure 4.8.

Figure 4.8 *An example of a GF(2^2) field*

Addition

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

Identity: 00

Multiplication

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

Identity: 01

Group

A group G, sometimes 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.

Primitive Roots

- A very interesting concept in multiplicative group is that of primitive root, which is used in the **ElGamal cryptosystem.**
- In the group $G = \langle Z_n^*, * \rangle$, when the order of an element is the same as $\phi(n)$, that element is called the **primitive root** of the group.
- **Order of the Group:** Number of elements in the group G.
- **Order of an Element, ord(a):** The order of an element, a, is the smallest integer i such that $a^i \equiv e \pmod{n}$. The identity element e is 1 in this case.

Primitive Roots

Example 9.50

Table 9.5 shows the result of $a^i \equiv x \pmod 7$ for the group $\mathbf{G} = \langle \mathbf{Z}_7^*, \times \rangle$. In this group, $\phi(7) = 6$.

Table 9.5 *Example 9.50*

	$i = 1$	$i = 2$	$i = 3$	$i = 4$	$i = 5$	$i = 6$
$a = 1$	x: 1	x: 1	x: 1	x: 1	x: 1	x: 1
$a = 2$	x: 2	x: 4	x: 1	x: 2	x: 4	x: 1
Primitive root → $a = 3$	x: 3	x: 2	x: 6	x: 4	x: 5	x: 1
$a = 4$	x: 4	x: 2	x: 1	x: 4	x: 2	x: 1
Primitive root → $a = 5$	x: 5	x: 4	x: 6	x: 2	x: 3	x: 1
$a = 6$	x: 6	x: 1	x: 6	x: 1	x: 6	x: 1

Primitive Roots

- The orders of elements are ord(1) = 1, ord(2) = 3, ord(3) = 6, ord(4) = 3, ord(5) = 6, and ord(6) = 1.
- Table 9.5 shows that only two elements, 3 and 5, have the order at $i = \phi(n) = 6$.
- Therefore, this group has only two primitive roots: 3 and 5.

Primitive Roots

The group $G = \langle Z_n^*, \times \rangle$ has primitive roots only if n is $2, 4, p^t$, or $2p^t$.

Example 9.51

For which value of n, does the group $\mathbf{G} = \langle \mathbf{Z}_n^*, \times \rangle$ have primitive roots: 17, 20, 38, and 50?

Solution

a. $\mathbf{G} = \langle \mathbf{Z}_{17}^*, \times \rangle$ has primitive roots, because 17 is a prime (p^t where t is 1).

b. $\mathbf{G} = \langle \mathbf{Z}_{20}^*, \times \rangle$ has no primitive roots.

c. $\mathbf{G} = \langle \mathbf{Z}_{38}^*, \times \rangle$ has primitive roots, because $38 = 2 \times 19$ and 19 is a prime.

d. $\mathbf{G} = \langle \mathbf{Z}_{50}^*, \times \rangle$ has primitive roots, because $50 = 2 \times 5^2$ and 5 is a prime.

Primitive Roots

If the group $G = \langle Z_n^*, \times \rangle$ has any primitive root, the number of primitive roots is $\phi(\phi(n))$.

For $G = \langle Z_7^*, * \rangle$, number of primitive roots is $\phi(\phi(7))=\phi(6)=2$.

Cyclic Group: if the group $G = \langle Z_n^*, \times \rangle$ has primitive roots, it is cyclic.

Each primitive root is a generator and can be used to create the whole set. In other words, if g is a primitive root in the group, we can generate the set Z_n^* as

$$\mathbf{Z}_n^* = \{g^1, g^2, g^3, \ldots, g^{\phi(n)}\}$$

Primitive Roots

Example 9.52

The group $\mathbf{G} = \langle \mathbf{Z}_{10}^*, \times \rangle$ has two primitive roots because $\phi(10) = 4$ and $\phi(\phi(10)) = 2$. It can be found that the primitive roots are 3 and 7. The following shows how we can create the whole set $\mathbf{Z}_{10}^*$ using each primitive root.

$$
\begin{array}{llllll}
g = 3 \rightarrow & g^1 \bmod 10 = 3 & g^2 \bmod 10 = 9 & g^3 \bmod 10 = 7 & g^4 \bmod 10 = 1 \\
g = 7 \rightarrow & g^1 \bmod 10 = 7 & g^2 \bmod 10 = 9 & g^3 \bmod 10 = 3 & g^4 \bmod 10 = 1
\end{array}
$$

Note that the group $\mathbf{G} = \langle \mathbf{Z}_p^*, \times \rangle$ is always cyclic because p is a prime.

The group $G = \langle Z_n^*, \times \rangle$ is a cyclic group if it has primitive roots.
The group $G = \langle Z_p^*, \times \rangle$ is always cyclic.

Primitive Roots

36. For the group $\mathbf{G} = \langle \mathbf{Z}_{19}^*, \times \rangle$:
    a. Find the order of the group.
    b. Find the order of each element in the group.
    c. Find the number of primitive roots in the group.
    d. Find the primitive roots in the group.
    e. Show that the group is cyclic.

Quadratic Residues

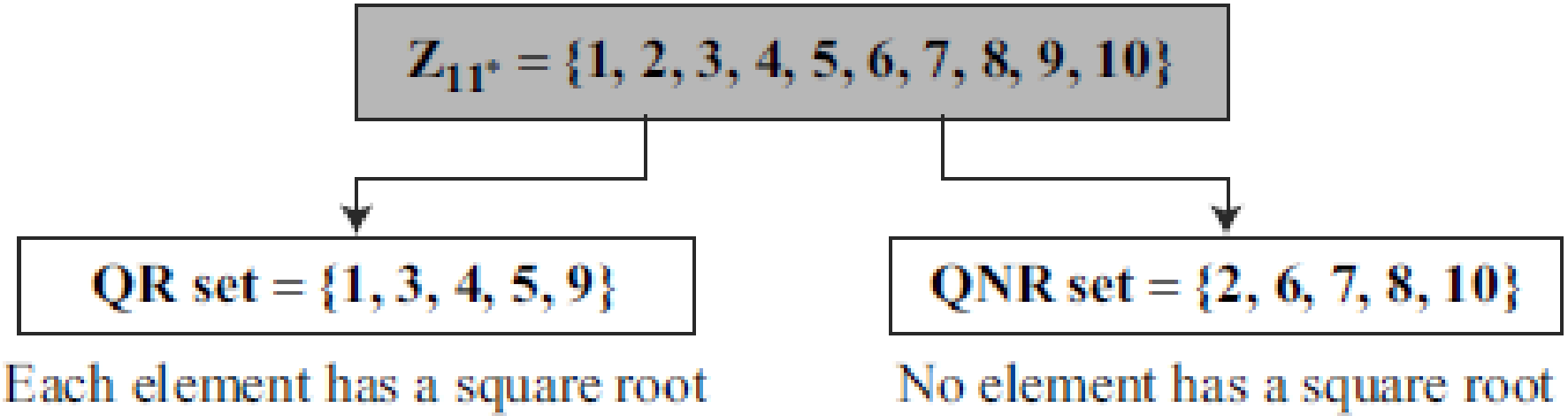
In the equation $x^2 \equiv a \pmod{p}$, a is called a **quadratic residue (QR)** if the equation has two solutions; a is called **quadratic nonresidue (QNR)** if the equation has no solutions.

It can be proved that in Z_p^*, with $p - 1$ elements, exactly $(p - 1)/2$ elements are quadratic residues and $(p - 1)/2$ are quadratic nonresidues.

If a is a square mod n, we say that a is a quadratic residue mod n. If not, a is a quadratic nonresidue.

Quadratic Residues

Figure 9.4 *Division of $\mathbf{Z}_{11}$* elements into QRs and QNRs*



Quadratic Residues

Proposition 13.1. *Let p be an odd prime and let $a \not\equiv 0 \pmod{p}$. Then $a^{(p-1)/2} \equiv \pm 1 \pmod{p}$. Moreover,*

$$a \text{ is a square mod } p \iff a^{(p-1)/2} \equiv 1 \pmod{p}.$$

Proof. Let $b \equiv a^{(p-1)/2} \pmod{p}$. Then $b^2 \equiv a^{p-1} \equiv 1 \pmod{p}$ by Fermat's theorem. By Corollary 6.11, $b \equiv \pm 1 \pmod{p}$, so $a^{(p-1)/2} \equiv \pm 1 \pmod{p}$.

If a is a square mod p, we have $x^2 \equiv a$ for some x, so

$$a^{(p-1)/2} \equiv (x^2)^{(p-1)/2} \equiv x^{p-1} \equiv 1 \pmod{p},$$

Legendre symbol

Definition 13.2. *Let p be an odd prime and let a be an integer with $a \not\equiv 0 \pmod{p}$. Define the* **Legendre symbol**

$$\left(\frac{a}{p}\right) = \begin{cases} +1 & \text{if } x^2 \equiv a \pmod{p} \text{ has a solution} \\ -1 & \text{if } x^2 \equiv a \pmod{p} \text{ has no solution.} \end{cases}$$

Eg: (a/p)= (1/11)=+1, (2/11)=-1, (3/11)=+1

Proposition 13.3. *Let p be an odd prime and let $a, b \not\equiv 0 \pmod{p}$. Then*

(a) (Euler's Criterion)

$$\left(\frac{a}{p}\right) \equiv a^{(p-1)/2} \pmod{p}.$$

(b)

$$\left(\frac{a}{p}\right)\left(\frac{b}{p}\right) = \left(\frac{ab}{p}\right).$$

(c) If $a \equiv b \pmod{p}$ then $\left(\frac{a}{p}\right) = \left(\frac{b}{p}\right)$.

(d)

$$\left(\frac{-1}{p}\right) = \begin{cases} +1 & \text{if } p \equiv 1 \pmod{4} \\ -1 & \text{if } p \equiv 3 \pmod{4}. \end{cases}$$

Theorem 13.4. *(Quadratic Reciprocity) (a) Let p and q be distinct odd primes. Then*

$$\left(\frac{q}{p}\right) = (-1)^{(p-1)(q-1)/4}\left(\frac{p}{q}\right).$$

In other words,

$$\left(\frac{q}{p}\right) = \begin{cases} \left(\frac{p}{q}\right) & \text{if at least one of } p, q \text{ is } 1 \pmod 4 \\ -\left(\frac{p}{q}\right) & \text{if } p \equiv q \equiv 3 \pmod 4. \end{cases}$$

(b) Let p be an odd prime. Then

$$\left(\frac{-1}{p}\right) = (-1)^{(p-1)/2} = \begin{cases} +1 \text{ if } p \equiv 1 \pmod 4 \\ -1 \text{ if } p \equiv 3 \pmod 4. \end{cases}$$

(c) Let p be an odd prime. Then

$$\left(\frac{2}{p}\right) = (-1)^{(p^2-1)/8} = \begin{cases} +1 \text{ if } p \equiv 1, 7 \pmod 8 \\ -1 \text{ if } p \equiv 3, 5 \pmod 8. \end{cases}$$

Jacobi Symbol

Let m be a positive odd integer. Write the prime factorization of m as

$$m = p_1^{a_1} p_2^{a_2} \cdots p_r^{a_r}.$$

Let $\gcd(b, m) = 1$. Define the **Jacobi symbol**

$$\left(\frac{b}{m}\right) = \left(\frac{b}{p_1}\right)^{a_1} \left(\frac{b}{p_2}\right)^{a_2} \cdots \left(\frac{b}{p_r}\right)^{a_r},$$

where $\left(\frac{b}{p_i}\right)$ is the Legendre symbol. For example,

Jacobi Symbol

Example:

$$\left(\frac{2}{15}\right) = \left(\frac{2}{3}\right)\left(\frac{2}{5}\right) = (-1)(-1) = +1.$$

Since 2 is not a square mod 3, it cannot be a square mod 15. Therefore, we issue the following:

Warning: $(b/m) = +1$ does not imply that b is a square mod m.

Theorem 13.8. *(Reciprocity for Jacobi symbols) Let m, n be positive odd integers with* $\gcd(m,n) = 1$.

(a)

$$\left(\frac{m}{n}\right) = (-1)^{(m-1)(n-1)/4} \left(\frac{n}{m}\right).$$

In other words,

$$\left(\frac{m}{n}\right) = \begin{cases} \left(\frac{n}{m}\right) & \text{if at least one of } m, n \text{ is } 1 \pmod 4 \\ -\left(\frac{n}{m}\right) & \text{if } m \equiv n \equiv 3 \pmod 4. \end{cases}$$

(b) (Supplementary Law for -1)

$$\left(\frac{-1}{m}\right) = (-1)^{(m-1)/2} = \begin{cases} +1 \ \textit{if}\ m \equiv 1 \pmod 4 \\ -1 \ \textit{if}\ m \equiv 3 \pmod 4. \end{cases}$$

(c) (Supplementary Law for 2)

$$\left(\frac{2}{m}\right) = (-1)^{(m^2-1)/8} = \begin{cases} +1 \ \textit{if}\ m \equiv 1,7 \pmod 8 \\ -1 \ \textit{if}\ m \equiv 3,5 \pmod 8. \end{cases}$$

Gauss's Lemma

Lemma 13.9. *(Gauss's Lemma) Let p be an odd prime and let $a \not\equiv 0 \pmod{p}$. Let n be the number of integers in the set*

$$\{a, 2a, 3a, \ldots, (p-1)a/2\}$$

that are congruent to an integer between $p/2$ and p. Then

$$\left(\frac{a}{p}\right) = (-1)^n.$$

Proof: