MATHEMATICS OF SYMMETRIC KEY CRYPTOGRAPHY

Presentation by:
V. Balasubramanian
SSN College of Engineering

Objectives

- Algebraic structures
- Modular arithmetic
- Euclid“s algorithm
- Congruence and matrices
- Groups, Rings, Fields- Finite fields

Objectives

- To review integer arithmetic, concentrating on divisibility and finding the greatest common divisor using the Euclidean algorithm
- To understand how the extended Euclidean algorithm
- To emphasize the importance of modular arithmetic and the modulo operator, because they are extensively used in cryptography

Introduction

- Number theory is pervasive in cryptographic algorithms.

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

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

Example

The positive divisors of 24 are $1, 2, 3, 4, 6, 8, 12$, and 24.

$13 \mid 182;\ -5 \mid 30;\ 17 \mid 289;\ -3 \mid 33;\ 17 \mid 0$

$11 \mid 66$ and $66 \mid 198 \Rightarrow 11 \mid 198$

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

$7 \mid 14$ and $7 \mid 63$.

To show $7 \mid (3 \times 14 + 2 \times 63)$,

we have $(3 \times 14 + 2 \times 63) = 7(3 \times 2 + 2 \times 9)$,
and it is obvious that $7 \mid (7(3 \times 2 + 2 \times 9))$.

Divisibility Property

- 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 $mg + nh$

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

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:

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

Division

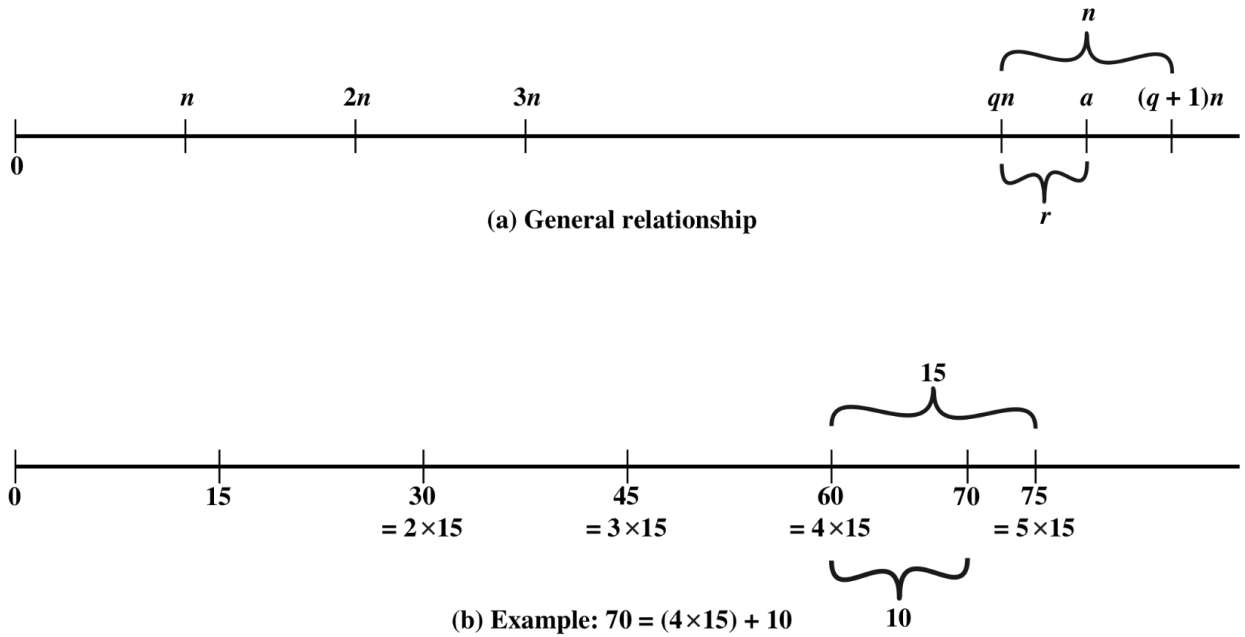


Figure 4.1 The Relationship $a = qn + r$; $0 \leq r < n$

Euclid's Theorem

- 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

- 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, $\gcd(a,b) = \gcd(|a|, |b|)$

- 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 $\gcd(a,b) = 1$

Algorithm

GCD(a,b):

```
A=a, B=b
  while B>0
      R = A mod B
      A = B, B = R
  return A
```

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)

GCD(2740,1760)

q	r_1	r_2	r
1	2740	1760	980
1	1760	980	780
1	980	780	200
3	780	200	180
1	200	180	20
9	180	20	0
	20	0	

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:*

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

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

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

Negative number modulo k = k minus positive number modulo k. To find (–n)%k = k–(n%k)

Modular Arithmetic

- Congruent modulo *n*
  - Two integers *a* and *b* are said to be **congruent modulo *n*** if $(a \bmod n) = (b \bmod n)$
  - This is written as $a = b \pmod{n}$[2]
  - Note that if $a = 0 \pmod{n}$, then $n \mid a$

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

Properties of Congruence

- Congruences have the following properties:

  1. $a = b \pmod{n}$ if $n \mid (a - b)$

  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 $n \mid (a - b)$, 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:

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

Examples

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

Exponentiation is performed by repeated multiplication

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

$$11^2 = 121 \equiv 4 \pmod{13}$$
$$11^4 = (11^2)^2 \equiv 4^2 \equiv 3 \pmod{13}$$
$$11^7 \equiv 11 \times 4 \times 3 \equiv 132 \equiv 2 \pmod{13}$$

Arithmetic Modulo 8

Table 2.2 Arithmetic Modulo 8

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

(a) Addition modulo 8

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

(b) Multiplication modulo 8

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

(c) Additive and multiplicative inverse modulo 8

Set of Residues

Define the set Z_n as the set of nonnegative integers less than n:

$$Z_n = \{0, 1, \ldots, (n-1)\}$$

This is referred to as the **set of residues**, or **residue classes** (mod n). To be more precise, each integer in Z_n represents a residue class. We can label the residue classes (mod n) as $[0], [1], [2], \ldots, [n-1]$, where

$$[r] = \{a: a \text{ is an integer}, a \equiv r \pmod{n}\}$$

The residue classes (mod 4) are

$[0] = \{\ldots, -16, -12, -8, -4, 0, 4, 8, 12, 16, \ldots\}$

$[1] = \{\ldots, -15, -11, -7, -3, 1, 5, 9, 13, 17, \ldots\}$

$[2] = \{\ldots, -14, -10, -6, -2, 2, 6, 10, 14, 18, \ldots\}$

$[3] = \{\ldots, -13, -9, -5, -1, 3, 7, 11, 15, 19, \ldots\}$

Properties of Modular Arithmetic for Integers in Z_n

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

Modular Arithmetic

if $(a + b) \equiv (a + c) \pmod{n}$ **then** $b \equiv c \pmod{n}$ **(4.4)**

$$(5 + 23) \equiv (5 + 7) \pmod{8};\ 23 \equiv 7 \pmod{8}$$

if $(a \times b) \equiv (a \times c) \pmod{n}$ **then** $b \equiv c \pmod{n}$ **if** a is relatively prime to n **(4.5)**

Recall that two integers are **relatively prime** if their only common positive integer factor is 1. Similar to the case of Equation (4.4), we can say that Equation (4.5) is

$$\begin{aligned} ((a^{-1})ab) &\equiv ((a^{-1})ac) \pmod{n} \\ b &\equiv c \pmod{n} \end{aligned}$$

Example

To see this, consider an example in which the condition of Equation (4.5) does not hold. The integers 6 and 8 are not relatively prime, since they have the common factor 2. We have the following:

$$6 \times 3 = 18 \equiv 2 \pmod{8}$$
$$6 \times 7 = 42 \equiv 2 \pmod{8}$$

Yet $3 \not\equiv 7 \pmod{8}$.

Euclid's Algorithm

$$\gcd(a, b) = \gcd(b, a \bmod b)$$

$$\gcd(55, 22) = \gcd(22, 55 \bmod 22) = \gcd(22, 11) = 11$$

Extended Euclid's Algorithm

- The extended Euclidean algorithm not only calculate the greatest common divisor *d but also two additional integers x* and *y that satisfy the following equation.*
- *It is whole numbers – cannot tolerate fractions*

Example

Example 1: $m = 65, n = 40$

Step 1: The (usual) Euclidean algorithm:

$$
\begin{aligned}
(1) \qquad 65 &= 1 \cdot 40 + \boxed{25} \\
(2) \qquad 40 &= 1 \cdot \boxed{25} + 15 \\
(3) \qquad \boxed{25} &= 1 \cdot 15 + 10 \\
(4) \qquad 15 &= 1 \cdot 10 + 5 \\
10 &= 2 \cdot 5
\end{aligned}
$$

Therefore: $\gcd(65, 40) = 5$.

Example

Step 2: Using the method of back-substitution:

$$\begin{aligned} 5 &\overset{(4)}{=} 15 - 10 \\ &\overset{(3)}{=} 15 - (25 - 15) && = 2 \cdot 15 - 25 \\ &\overset{(2)}{=} 2(40 - 25) - 25 && = 2 \cdot 40 - 3 \cdot 25 \\ &\overset{(1)}{=} 2 \cdot 40 - 3(65 - 40) && = 5 \cdot 40 - 3 \cdot 65 \end{aligned}$$

Conclusion: $65(-3) + 40(5) = 5$.

Example

Example 2: $m = 1239, n = 735$

Step 1: The (usual) Euclidean algorithm:

$$
\begin{aligned}
(1) \qquad 1239 &= 1 \cdot 735 + \boxed{504} \\
(2) \qquad 735 &= 1 \cdot \boxed{504} + 231 \\
(3) \qquad \boxed{504} &= 2 \cdot 231 + 42 \\
(4) \qquad 231 &= 5 \cdot 42 + 21 \\
42 &= 2 \cdot 21
\end{aligned}
$$

Therefore: $\gcd(1239, 735) = 21$.

Contd…

Step 2: Using the method of back-substitution:

$$
\begin{aligned}
21 &\overset{(4)}{=} 231 - 5 \cdot 42 \\
&\overset{(3)}{=} 231 - 5(504 - 2 \cdot 231) && = 11 \cdot 231 - 5 \cdot 504 \\
&\overset{(2)}{=} 11(735 - 504) - 5 \cdot 504 && = 11 \cdot 735 - 16 \cdot 504 \\
&\overset{(1)}{=} 11 \cdot 735 - 16(1239 - 735) && = 27 \cdot 735 - 16 \cdot 1239
\end{aligned}
$$

Conclusion: $1239(-16) + 735(27) = 21$.

Example

- Find the inverse of 15 mod 26.
- GCD(26,15) = GCD(15,11) = GCD(11,4) = GCD(4,3) =GCD(3,1)= GCD(1,0) =1 Co-prime.
- Extended Euclidean algorithm.
- 26 = 1*26 + 0*15
- 15 = 0*26 + 1*15

Example

- 11 = Equ 1 – Equ 2 = 1 * 26 – 1*15
- 4 = Equ 2 – Equ 3 = -1 * 26 + 2* 15
- 3 = Equ3 – 2 * Equ 4 = 3*26 -5*15
- 1 = Equ 4 – Equ 5 = -4 *26 + 7 *15.
- Co-efficient is inverse. i.e., 7.

H.W

- Given a = 161 and b = 28, find gcd (a, b) and the values of s and t.

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

$$a = p_1^{a1} * p_2^{a2} * \ldots * p_{p1}^{a1}$$

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

Prime Numbers

$$91 = 7 \times 13$$
$$3600 = 2^4 \times 3^2 \times 5^2$$
$$11011 = 7 \times 11^2 \times 13$$

$$a = \prod_{p \in \mathrm{P}} p^{a_p} \quad \text{where each } a_p \geq 0$$

The integer 12 is represented by $\{a_2 = 2, a_3 = 1\}$.
The integer 18 is represented by $\{a_2 = 1, a_3 = 2\}$.
The integer 91 is represented by $\{a_7 = 1, a_{13} = 1\}$.

Prime Numbers

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

If $a \mid b$, then $a_p \leq b_p$ for all p.

$a = 12; b = 36; 12 \mid 36$

$12 = 2^2 \times 3; 36 = 2^2 \times 3^2$

$a_2 = 2 = b_2$

$a_3 = 1 \leq 2 = b_3$

Thus, the inequality $a_p \leq b_p$ is satisfied for all prime numbers.

Fermat and Euler Theorem

- Public-key cryptography uses Fermat's theorem and Euler's theorem.

Example

- Compute a^b mod N.
- a^b, $||a^b|| = O(b.||a||)$
- naive algorithm - does not run in polynomial time,
- but with a little bit of cleverness you can come up with an algorithm that does run in polynomial time.

Naive Algorithm

- Consider the following algorithm:

```
exp(a, b, N) {
    // assume b ≥ 0
    ans = 1;
    for (i=1, i ≤ b; i++)
        ans = [ans * a mod N];
    return ans;
}
```

Efficient Algorithm

Assume $b = 2^k$ for simplicity

- The preceding algorithm roughly corresponds to computing $a*a*a*\ldots*a$
- Better: compute $(((a^2)^2)^2\ldots)^2$
- 2^k multiplications vs. k squarings
  - Note $k = O(\|b\|)$

Contd…

```
exp(a, b, N) {
    // assume b ≥ 0
    x=a, t=1;
    while (b>0) {
        if (b odd)
            t = [t * x mod N], b = b-1;
        x = [x^2 mod N],  b = b/2; }
    return t; }
```

If b is odd, in first step subtract by 1,
then it becomes even.

Fermat's Theorem

- States the following:
  - If *p* is prime and *a* is a positive integer not divisible by *p* then

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

- Sometimes referred to as Fermat's Little Theorem
- An alternate form is:
  - If *p* is prime and *a* is a positive integer then

$$a^{p} = a \pmod{p}$$

- Plays an important role in public-key cryptography

Fermats Theorem

Theorem: (Fermat). If p is a prime and a is any number not divisible by p, then

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

For example, we know from this, without calculating, that $3^{22} \equiv 1 \bmod 23$.

It's more convenient to prove

$$a^p \equiv a \bmod p \text{ for all } a.$$

This clearly follows from the above congruence by multiplying it by a. And Fermat's little theorem follows from this congruence by canceling a which is allowed if p does not divide a.

The proof uses the binomial theorem. Clearly, $1^p \equiv 1 \bmod p$. Now

$$2^p = (1+1)^p = 1 + \binom{p}{1} + \binom{p}{2} + \cdots + \binom{p}{p-1} + 1 \equiv 1+0+0+\cdots+0+1 = 2 \bmod p.$$

Once we have $2^p \equiv 2 \bmod p$, we use the binomial theorem again to find 3^p:

$$3^p = (1+2)^p = 1 + \binom{p}{1}2 + \binom{p}{2}2^2 + \cdots + \binom{p}{p-1}2^{p-1} + 2^p \equiv 1+0+0+\cdots+0+2 = 3 \bmod p.$$

This process can be continued indefinitely to prove the result. (Technically, the result $a^p \equiv a \bmod p$ is found by induction on a.)

Proof

Proof: Consider the set of positive integers less than p: $\{1, 2, \ldots, p-1\}$ and multiply each element by a, modulo p, to get the set $X = \{a \bmod p, 2a \bmod p, \ldots, (p-1)a \bmod p\}$. None of the elements of X is equal to zero because p does not divide a. Furthermore, no two of the integers in X are equal. To see this,

are all positive integers with no two elements equal. We can conclude the X consists of the set of integers $\{1, 2, \ldots, p-1\}$ in some order. Multiplying the numbers in both sets (p and X) and taking the result mod p yields

$$a \times 2a \times \cdots \times (p-1)a \equiv [(1 \times 2 \times \cdots \times (p-1)] \pmod{p}$$
$$a^{p-1}(p-1)! \equiv (p-1)! \pmod{p}$$

Example

$$a = 7, p = 19$$
$$7^2 = 49 \equiv 11 \pmod{19}$$
$$7^4 \equiv 121 \equiv 7 \pmod{19}$$
$$7^8 \equiv 49 \equiv 11 \pmod{19}$$
$$7^{16} \equiv 121 \equiv 7 \pmod{19}$$
$$a^{p-1} = 7^{18} = 7^{16} \times 7^2 \equiv 7 \times 11 \equiv 1 \pmod{19}$$

$2^{16}\ mod\ 17$

$p = 5, a = 3 \quad a^p = 3^5 = 243 \equiv 3 \pmod 5 = a \pmod p$

$p = 5, a = 10 \quad a^p = 10^5 = 100000 \equiv 10 \pmod 5 \equiv 0 \pmod 5 = a \pmod p$

Fermat's Theorem

- If *p is prime and a is a* positive integer $a^p \equiv a \pmod{p}$

$p = 5, a = 3 \quad a^p = 3^5 = 243 \equiv 3 \pmod{5} = a \pmod{p}$

$p = 5, a = 10 \quad a^p = 10^5 = 100000 \equiv 10 \pmod{5} \equiv 0 \pmod{5} = a \pmod{p}$

Example

we can define the mod operator as: $a \bmod n = a - n \times \lfloor a/n \rfloor$.

a. $5 \bmod 3 = 5 - 3 \lfloor 5/3 \rfloor = 2$

b. $5 \bmod -3 = 5 - (-3) \lfloor 5/(-3) \rfloor = -1$

c. $-5 \bmod 3 = -5 - 3 \lfloor (-5)/3 \rfloor = 1$

d. $-5 \bmod -3 = -5 - (-3) \lfloor (-5)/(-3) \rfloor = -2$

Example

- $3^{201} mod\ 11$

Use Fermat's theorem to find a number a between 0 and 72 with a congruent to 9794 modulo 73.

Use Fermat's theorem to find a number x between 0 and 28 with x^{85} congruent to 6 modulo 29. (You should not need to use any brute-force searching.)

Solution

Fermat's Theorem states that if p is prime and a is a positive integer not divisible by p, then $a^{p-1} \equiv 1 \pmod{p}$. Therefore $3^{10} \equiv 1 \pmod{11}$. Therefore

$3^{201} = (3^{10})^{20} \times 3 \equiv 3 \pmod{11}$.

12
6

Example

- Why is gcd(*n, n + 1) = 1 for two consecutive integers n and n + 1?*

If p were any prime dividing n and $n + 1$ it would also have to divide

$$(n + 1) - n = 1$$

Example

- **5555 to the power of 2222 + 2222 to the power of 5555 is divisible by 7?**
- $5555^{2222} + 2222^{5555} mod\ 7$
- 2222^1(mod 7) ≡ 3^1 ≡ 3
  2222^2(mod 7) ≡ 3^2 ≡ 2
  2222^3(mod 7) ≡ 3^3 ≡ 6
  2222^4(mod 7) ≡ 3^4 ≡ 4
  2222^5(mod 7) ≡ 3^5 ≡ 5
  2222^6(mod 7) ≡ 3^6 ≡ 1
  2222^7(mod 7) ≡ 3^7 ≡ 3

Contd…

- $5555^1 \pmod 7 \equiv 4^1 \equiv 4$
  $5555^2 \pmod 7 \equiv 4^2 \equiv 2$
  $5555^3 \pmod 7 \equiv 4^3 \equiv 1$
  $5555^4 \pmod 7 \equiv 4^4 \equiv 4$

Euler Totient Function

- Euler's totient function, written $\phi(n)$, *is the number of positive integers* less than *n and relatively prime to n.*

Before presenting Euler's theorem, we need to introduce an important quantity in number theory, referred to as **Euler's totient function**, written $\phi(n)$, and defined as the number of positive integers less than n and relatively prime to n. By convention, $\phi(1) = 1$.

DETERMINE $\phi(37)$ AND $\phi(35)$.

Because 37 is prime, all of the positive integers from 1 through 36 are relatively prime to 37. Thus $\phi(37) = 36$.

To determine $\phi(35)$, we list all of the positive integers less than 35 that are relatively prime to it:

1, 2, 3, 4, 6, 8, 9, 11, 12, 13, 16, 17, 18
19, 22, 23, 24, 26, 27, 29, 31, 32, 33, 34

There are 24 numbers on the list, so $\phi(35) = 24$.

$$\phi(p) = p - 1$$

Euler Totient Function

Now suppose that we have two prime numbers p and q with $p \neq q$. Then we can show that, for $n = pq$,

$$\phi(n) = \phi(pq) = \phi(p) \times \phi(q) = (p - 1) \times (q - 1)$$

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

where the 12 integers are $\{1, 2, 4, 5, 8, 10, 11, 13, 16, 17, 19, 20\}$.

Example

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

Euler's Theorem

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

Euler's Theorem

$a = 3; n = 10; \phi(10) = 4\ a^{\phi(n)} = 3^4 = 81 = 1 \pmod{10} = 1 \pmod{n}$
$a = 2; n = 11; \phi(11) = 10\ a^{\phi(n)} = 2^{10} = 1024 = 1 \pmod{11} = 1 \pmod{n}$

$$a^{\phi(n)+1} \equiv a \pmod{n}$$

Euler's Theorem

Prove the following: If p is prime, then $\phi(p^i) = p^i - p^{i-1}$. *Hint:* What numbers have a factor in common with p^i?

Only multiples of p have a factor in common with p^n, when p is prime. There are just p^{n-1} of these $\leq p^n$, so $\phi(p^n) = p^n - p^{n-1}$.

a. $\phi(41)$ b. $\phi(27)$ c. $\phi(231)$ d. $\phi(440)$

$\phi(41) = 40$, because 41 is prime
$\phi(27) = \phi(3^3) = 3^3 - 3^2 = 27 - 9 = 18$
$\phi(231) = \phi(3) \times \phi(7) \times \phi(11) = 2 \times 6 \times 10 = 120$
$\phi(440) = \phi(2^3) \times \phi(5) \times \phi(11) = (2^3 - 2^2) \times 4 \times 10 = 160$

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") ;

Contd...

```
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 mod n = 1 then return("inconclusive");
4. for j = 0 to k − 1 do
5. if a^(2^j q) mod n = n − 1 then return("inconclusive");
6. return("composite");
```

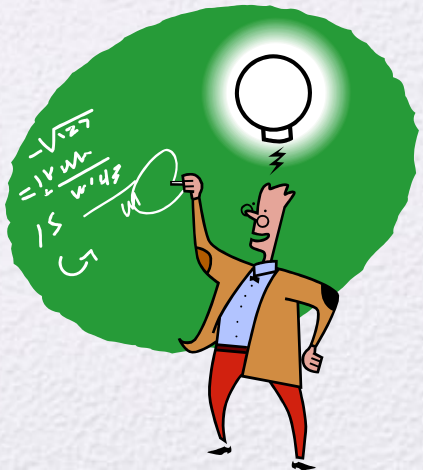
Contd...

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.

Now let us apply the test to the composite number $n = 13 \times 17 = 221$. 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-Rabin 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*

Example

What's x such that:

$x \equiv 2 \pmod 3$

$x \equiv 3 \pmod 5$

$x \equiv 2 \pmod 7$?

(So, $a_1 = 2$, etc. and $m_{1=3}$ etc.)

$m = m_1 \cdot \ldots \cdot m_n$.

$M_i = m / m_i$

$y_i M_i \equiv 1 \pmod{m_i}$.

Using the Chinese Remainder theorem:

$x = \Sigma_i a_i y_i M_i$

- $m = 3 \times 5 \times 7 = 105$
- $M_1 = m/3 = 105/3 = 35$
- 2 is an inverse of $M_1 = 35 \pmod 3$ (since $35 \times 2 \equiv 1 \pmod 3$)
- $M_2 = m/5 = 105/5 = 21$
- 1 is an inverse of $M_2 = 21 \pmod 5$ (since $21 \times 1 \equiv 1 \pmod 5$)
- $M_3 = m/7 = 15$
- 1 is an inverse of $M_3 = 15 \pmod 7$ (since $15 \times 1 \equiv 1 \pmod 7$)
- So , $x \equiv 2 \times 2 \times 35 + 3 \times 1 \times 21 + 2 \times 1 \times 15 = 233 \equiv 23 \pmod{105}$
- So answer: $x \equiv 23 \pmod{105}$

Table 8.3
Powers of Integers, Modulo 19

a	a^2	a^3	a^4	a^5	a^6	a^7	a^8	a^9	a^{10}	a^{11}	a^{12}	a^{13}	a^{14}	a^{15}	a^{16}	a^{17}	a^{18}
1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1
2	4	8	16	13	7	14	9	18	17	15	11	3	6	12	5	10	1
3	9	8	5	15	7	2	6	18	16	10	11	14	4	12	17	13	1
4	16	7	9	17	11	6	5	1	4	16	7	9	17	11	6	5	1
5	6	11	17	9	7	16	4	1	5	6	11	17	9	7	16	4	1
6	17	7	4	5	11	9	16	1	6	17	7	4	5	11	9	16	1
7	11	1	7	11	1	7	11	1	7	11	1	7	11	1	7	11	1
8	7	18	11	12	1	8	7	18	11	12	1	8	7	18	11	12	1
9	5	7	6	16	11	4	17	1	9	5	7	6	16	11	4	17	1
10	5	12	6	3	11	15	17	18	9	14	7	13	16	8	4	2	1
11	7	1	11	7	1	11	7	1	11	7	1	11	7	1	11	7	1
12	11	18	7	8	1	12	11	18	7	8	1	12	11	18	7	8	1
13	17	12	4	14	11	10	16	18	6	2	7	15	5	8	9	3	1
14	6	8	17	10	7	3	4	18	5	13	11	2	9	12	16	15	1
15	16	12	9	2	11	13	5	18	4	3	7	10	17	8	6	14	1
16	9	11	5	4	7	17	6	1	16	9	11	5	4	7	17	6	1
17	4	11	16	6	7	5	9	1	17	4	11	16	6	7	5	9	1
18	1	18	1	18	1	18	1	18	1	18	1	18	1	18	1	18	1

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

Summary

- Prime numbers
- Fermat's Theorem
- Euler's totient function
- Euler's Theorem
- Testing for primality
  - Miller-Rabin algorithm
  - A deterministic primality algorithm
  - Distribution of primes

- The Chinese Remainder Theorem
- Discrete logarithms
  - Powers of an integer, modulo *n*
  - Logarithms for modular arithmetic
  - Calculation of discrete logarithms

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

- Obeys CAIN:
  - Closure : a,b in S, then a.b in S
  - Associative law :(a.b).c = a.(b.c)
  - has Identity e :e.a = a.e = a
  - has Inverses a-1 :$a.a^{-1} = e$

- if commutative a.b = b.a
  - then forms an abelian group

If a group has a finite number of elements, it is referred to as a **finite group**, and the **order** of the group is equal to the number of elements in the group. Otherwise, the group is an **infinite group**.

A group is said to be **abelian** if it satisfies the following additional condition:

(A5) Commutative: $a \cdot b = b \cdot a$ for all a, b in G.

Example

- 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.

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

Example

$\mathbb{Z}_N = \{0, \ldots, N-1\}$ under addition modulo N

- Identity is 0
- Inverse of a is [-a mod N]
- Associativity, commutativity obvious
- Order N

- $m \cdot a = a + \cdots + a \bmod N$
  - Can be computed efficiently

Contd…

- Modular Inverses uses gcd, inverse of b mod N
- Gcd(b,N) =1.

Contd…

- If p is prime, then 1, 2, 3, …, p-1 are all invertible modulo p

- If N=pq for p, q distinct primes, then the invertible elements are the integers from 1 to N-1 that are *not* multiples of p or q

$\mathbb{Z}^*_N$ = invertible elements between 1 and N-1 under multiplication modulo N

- Closure not obvious, but can be shown
- Identity is 1
- Inverse of a is $[a^{-1} \bmod N]$
- Associativity, commutativity obvious

- $a^m = a \cdots a \bmod N$

Contd…

$\phi(N)$ = the number of invertible elements modulo N

$= |\{a \in \{1, \ldots, N-1\} : \gcd(a, N) = 1\}|$

= The order of $\mathbb{Z}^*_N$

– If N is prime, then $\phi(N) = N-1$

– If N=pq, p and q distinct primes, $\phi(N) = ?$

$\phi(21) = \phi(3) \times \phi(7) = (3-1) \times (7-1) = 2 \times 6 = 12$
where the 12 integers are $\{1, 2, 4, 5, 8, 10, 11, 13, 16, 17, 19, 20\}$.

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

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 $a\,1 = 1a = a$ 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

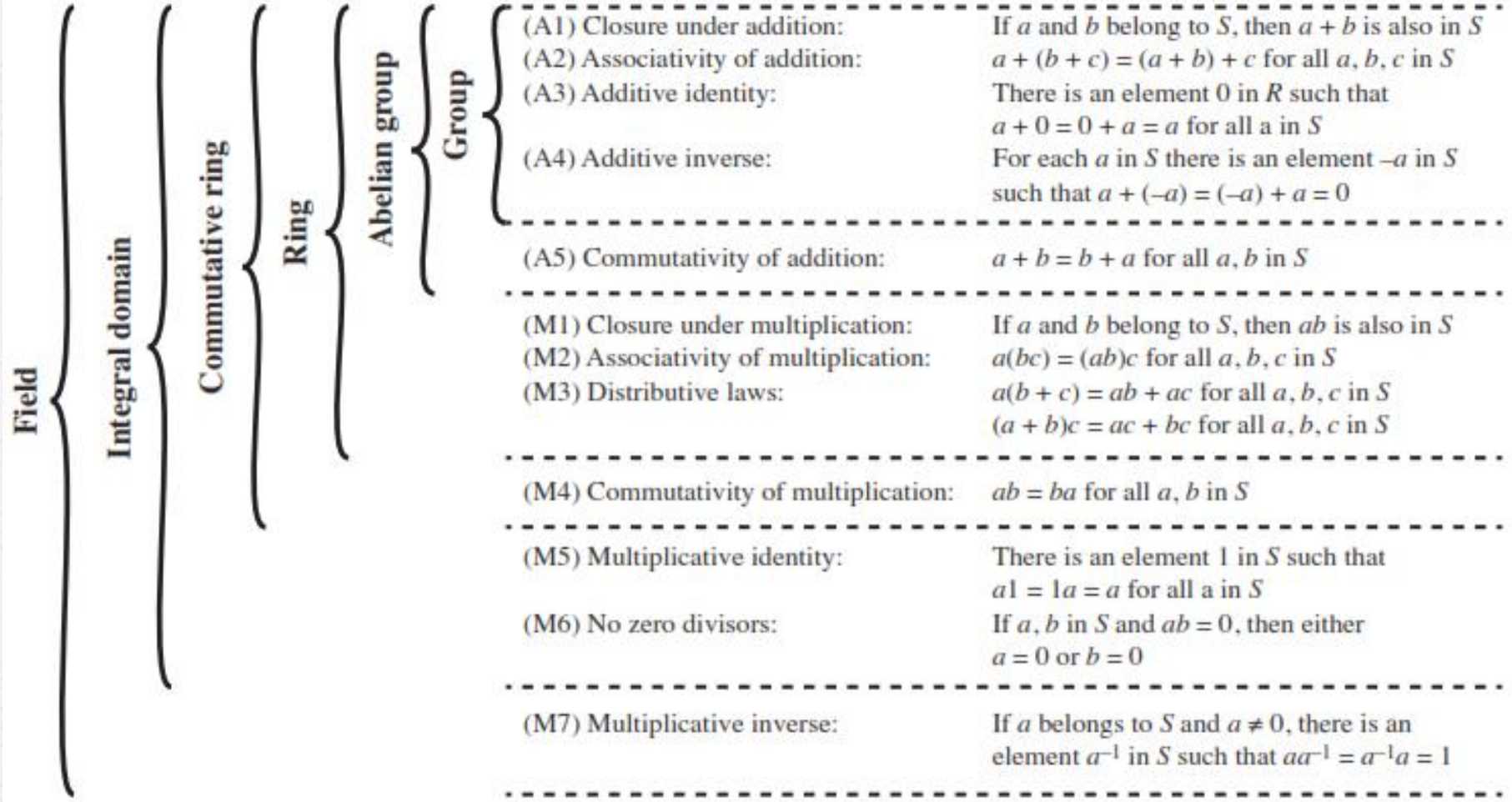
  (M7) Multiplicative inverse:

  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.

Contd...


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

Contd…

- 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; in fact, only the elements 1 and -1 have multiplicative inverses in the integers.

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

Table 4.5(a) 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

Table 4.5(b) 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

Table 4.5(c)

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

In this section, we have shown how to construct a finite field of order p, where p is prime.

GF(p) is defined with the following properties:

- 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
- We have shown that the elements of GF(p) are the integers $\{0, 1, \ldots, p-1\}$ 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

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

(a) Addition

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

(b) Subtraction

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

(c) Multiplication

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

(d) Division

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**

- The greatest common divisor of two integers is the largest positive integer that exactly _____ both integers.

- A) multiplies B) exponentially multiplies

- C) squares D) divides

- Two integers are _____ if their only common positive integer factor is 1.

- A) relatively prime
- B) congruent modulo
- C) polynomials
- D) residual

- The _____ of two numbers is the largest integer that divides both numbers.
- A) greatest common divisor B) prime polynomial
- C) lowest common divisor D) integral divisor

- A ring is said to be _____ if it satisfies the condition ab = ba for all a, b in R.

- A) cyclic
- B) commutative
- C) abelian
- D) infinite

- . A _____ is a set of elements on which two arithmetic operations have been defined and which has the properties of ordinary arithmetic, such as closure, associativity, commutativity, distributivity, and having both additive and multiplicative inverses.

- A) field
- B) modulus
- C) group
- D) ring

- A _____ is a field with a finite number of elements.
- A) finite group B) finite order
- C) finite field D) finite ring

- If b|a, we say that b is a _____ of a.
- A) residue
- B) group
- C) divisor
- D) modulus

- For given integers a and b, the extended _____ algorithm not only calculates the greatest common divisor d but also two additional integers x and y.

- A) modular
- B) Euclidean
- C) associative
- D) cyclic

- A group is said to be _____ if it satisfies the condition a * b = b * a for all a, b in G.
- A) abelian B) infinite
- C) cyclic D) commutative
-

- With the understanding that remainders are allowed, we can say that polynomial division is possible if the coefficient set is a _____ .

- A) ring
- B) field
- C) factor
- D) divisor

- By analogy to integers, an irreducible polynomial is also called a _____ .
- A) constant polynomial B) monic polynomial
- C) polynomial ring D) prime polynomial
-

- The congruence relation is used to define _____ .
- A) finite groups B) greatest common divisor
- C) lowest common divisor D) residue classes

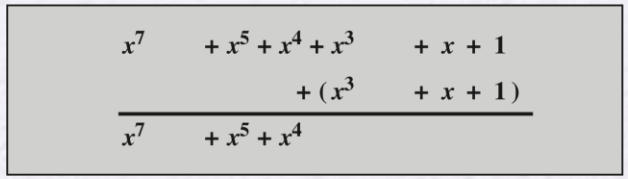
- As a _____ relation, mod expresses that two arguments have the same remainder with respect to a given modulus.

- A) finite
- B) monic
- C) congruence
- D) cyclic

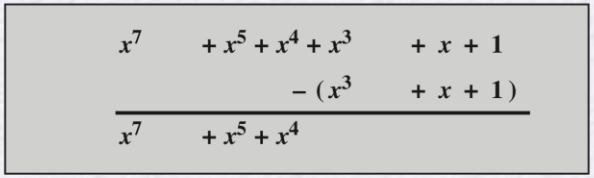
- . The order of a finite field must be of the form pn where p is a prime and n is a __ .
- A) identity element B) positive integer
- C) commutative ring D) associative

Example of Polynomial Arithmetic Over GF(2)

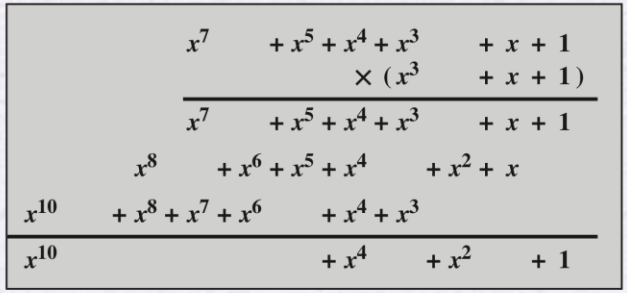
(Figure 4.4 can be found on page 110 in the textbook)



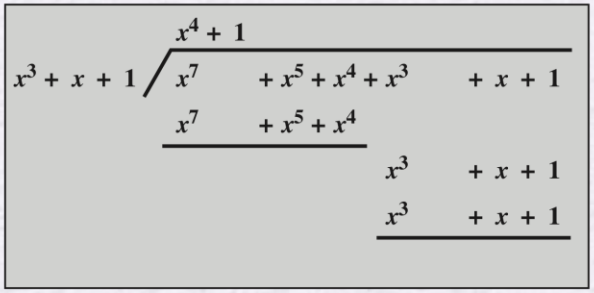
(a) Addition



(b) Subtraction



(c) Multiplication



(d) Division

Figure 4.4 Examples of Polynomial Arithmetic over GF(2)

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

Table 4.6(a) 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

Table 4.6(b) 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

Table 4.6(c)

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

Table 4.7 (page 117 in textbook)

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

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

(a) Addition

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

Table 4.8

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

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

(Table 4.8 can be found on page 118 in textbook)

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

Table 4.9

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

Table 4.10 (page 123 in textbook)

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

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

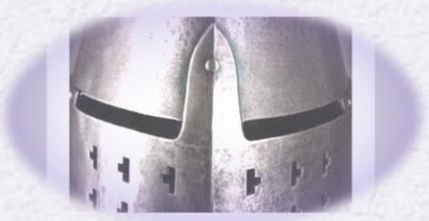
(a) Addition

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