Number Theory

Cryptography

Modular Arithmetic

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

$$a = qn + r \quad \text{where } q = \text{floor}(a/n)$$

a = 11;	**n = 7;**	**11 = 1 x 7 + 4;**	**r = 4**	**q = 1**
a = -11;	n = 7;	-11 = (-2) x 7 + 3;	r = 3	q = -2

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, we can always write:
- 11 mod 7 = 4
- −11 mod 7 = 3

$$a = \lfloor a/n \rfloor \times n + (a \bmod n)$$

congruent modulo

- Two integers a and b are said to be congruent modulo n, if (a mod n) = (b mod n). This is written as $a \equiv b \pmod{n}$.

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

Which is same as a-b=kn

For example,

$$38 \equiv 14 \pmod{12}$$

because $38 - 14 = 24$, which is a multiple of 12, or, equivalently, because both 38 and 14 have the same remainder 2 when divided by 12.

The same rule holds for negative values:

$$\begin{aligned} -8 &\equiv 7 \pmod{5} \\ 2 &\equiv -3 \pmod{5} \\ -3 &\equiv -8 \pmod{5}. \end{aligned}$$

Divisors

- We say that a nonzero b divides a if a = mb for some m, where a, b, and m are integers. That is, b divides a if there is no remainder on division.
- The notation is commonly used to mean b divides a. Also, if b|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.

Modular Arithmetic Operations

- By definition , the (mod n) operator maps all integers into the set of integers {0, 1,... (n – 1)}.
- This suggests the question: Can we perform arithmetic operations within the confines of this set?
- It turns out that we can; this technique is known as **modular arithmetic**.

Modular Arithmetic Operations

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. $[(a \bmod n) \times (b \bmod n)] \bmod n = (a \times b) \bmod n$

e.g.

[(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) x (15 mod 8)] mod 8 = 21 mod 8 = 5 (11 x 15) mod 8 = 165 mod 8 = 5

- Exponentiation is performed by repeated multiplication, as in ordinary arithmetic.

To find 11^7 mod 13, we can proceed as follows:

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

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

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

Modulo 8 Addition Example

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

Modulo 8 Multiplication

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

an illustration of modular addition and multiplication modulo 8

[View full size image]

+	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

×	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 inverses modulo 8

Properties of Modular Arithmetic

- 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 modulo n.
- To be more precise, each integer in Z_n represents a residue class. We can label the residue classes modulo n as [0], [1], [2],...,[n−1], where
- $[r] = \{a: a \text{ is an integer}, a \equiv r \pmod{n}\}$

- The residue classes modulo 4 are

$[0]_4 = \{ .. , -16, -12, -8, -4, 0, 4, 8, 12, 16,..\}$
$[1]_4 = \{ ... , -15, -11, -7, -3, 1, 5, 9, 13, 17, \}$
$[2]_4 = \{.., -14, -10, -6, -2, 2, 6, 10,14, 18, ... \}$
$[3]_4 = \{ ..,-13, -9, -5, -1, 3, 7, 11, 15, 19, ... \}$

Properties of Modular Arithmetic

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 $w + z \equiv 0 \bmod n$

Relative Prime(co-prime)

- Two integers 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

LCM and Greatest Common Divisor

- A nonzero b is defined to be a divisor of a if a = mb for some m, where a, b, and m are integers.
- We will use the notation gcd(a, b) to mean the **greatest common divisor** of a and b.
- The positive integer c is said to be the greatest common divisor of a and b if
  - c is a divisor of a and of b;
  - any divisor of a and b is a divisor of c.

- An equivalent definition is the following:
- gcd(a, b) = max[k, such that $k|a$ and $k|b$]

$$\operatorname{lcm}(a, b) = \frac{ab}{\gcd(a, b)}$$

For example, $\operatorname{lcm}(70, 130) = \frac{70 \cdot 130}{10} = 910$.

If two integers a and b share no common factors, then $\gcd(a, b) = 1$. Such a pair of integers are called **relatively prime**.

The Euclidean Algorithm

- The Euclidean algorithm is based on the following theorem: For any nonnegative integer a and any positive integer b,

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

- Example
- gcd(55, 22) = gcd(22, 55 mod 22) = gcd(22, 11) = 11.
- gcd(11, 10) = gcd(10, 1) = gcd(1, 0) = 1

- The Euclidean algorithm makes repeated use of above equation to determine the greatest common divisor, as follows. The algorithm assumes $a > b > 0$. It is acceptable to restrict the algorithm to positive integers because $\gcd(a, b) = \gcd(|a|, |b|)$.

EUCLID(a, b)

1. $A \leftarrow a$; $B \leftarrow b$.
2. if $B = 0$ return $A = \gcd(a, b)$
3. $R = A \bmod B$
4. $A \leftarrow B$
5. $B \leftarrow R$
6. goto 2

The algorithm has the following progression

$$A_1 = B_1 \times Q_1 + R_1$$

$$A_2 = B_2 \times Q_2 + R_2$$

$$A_3 = B_3 \times Q_3 + R_3$$

$$A_4 = B_4 \times Q_4 + R_4$$

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)

trace this algorithm on inputs a = 105 and b = 252

x	y	$r = \text{remainder}(x, y)$
105	252	105
252	105	42
105	42	21
42	21	0
21	0	

Finite Fields of The Form GF(p)

- Infinite fields are not of particular interest in the context of cryptography.
- However, finite fields play a crucial role in many cryptographic algorithms.
- It can be shown that the order of a finite field (number of elements in the field) must be a power of a prime p^n, where n is a positive integer.
- A prime number is an integer whose only positive integer factors are itself and 1. That is, 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)**; stands for Galois field, in honor of the mathematician who first studied finite fields.

Finite Fields of Order p

- For a given prime, p, the finite field of order p, GF(p) is defined as the set Z_p of integers {0, 1,..., p–1}, together with the arithmetic operations modulo p.
- The simplest finite field is GF(2). Its arithmetic operations are easily summarized:

+	0	1
0	0	1
1	1	0

Addition

×	0	1
0	0	0
1	0	1

Multiplication

$+$	0	1
0	0	1
1	1	0

$\times$	0	1
0	0	0
1	0	1

w	$-w$	w^{-1}
0	0	—
1	1	1

The simplest finite field is GF(2).

$\times$	0	1	2	3	4	5	6
0	0	0	0	0	0	0	0
1	0	1	2	3	4	5	6
2	0	2	4	6	1	3	5
3	0	3	6	2	5	1	4
4	0	4	1	5	2	6	3
5	0	5	3	1	6	4	2
6	0	6	5	4	3	2	1

GF(7)

(b) Multiplication modulo 7

Floor and ceiling functions

- In mathematics and computer science, the **floor** and **ceiling** functions map a real number to the largest previous or the smallest following integer, respectively.
- More precisely, floor(*x*) is the largest integer less than or equal to *x* and ceiling(*x*) is the smallest integer greater than or equal to *x*.
- For example,
  - **floor(2.4)=2**
  - **Ceiling(2.4)=3**

Floor(2)=?

ceiling(2)=? 2? Or something else??

Finding the Multiplicative Inverse in GF(p)

- If a and b are relatively prime, then b has a multiplicative inverse modulo a.
- That is, if $\gcd(a, b) = 1$, then b has a multiplicative inverse modulo a.
- That is, for positive integer $b < a$, there exists a $b^{-1} < a$ such that $bb^{-1} = 1 \bmod a$.
- If a is a prime number and $b < a$, then clearly a and b are relatively prime and have a greatest common divisor of 1.

Extended Eucledean Algorithm

- It is easy to find the multiplicative inverse of an element in GF(p) for small values of p.
- We simply construct a multiplication table, and the desired result can be read directly.
- However, for large values of p, this approach is not practical.
- The alternative is **Extended Eucledean Algorithm.**

Extended Eucledean 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 exists
3) If B3=1 return B3=gcd(m,b);B2=b^{-1} mod m
4) Q=floor(A3/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 step 2

Example

- shows that gcd(1759, 550) = 1 and that the multiplicative inverse of 550 is 355; that is,
- 550 x 355 ≡1 (mod 1759).

Finding the Multiplicative Inverse of 550 in GF(1759)

S.N.	Q	A1	A2	A3	B1	B2	B3	T1	T2	T3
1	–	1	0	1759	0	1	550			
2	3	0	1	550	1	–3	109	1	–3	109
3	5	1	–3	109	–5	16	5	–5	16	5
4	21	–5	16	5	106	–339	4	106	–339	4
5	1	106	–339	4	–111	355	1	–111	355	1

Prime Numbers

- An integer $p > 1$ is a prime number if and only if its only divisors are ± 1 and $\pm p$.
- Prime numbers play important role in computations involving numbers, including cryptographic computations.
- But how to test whether a number 'n' is prime or not , particularly if it is large.
- Testing all possible divisors of n is computationally infeasible for large 'n'.
- So we need different primality Testing algorithms.

Fermat's Theorem

- This is sometimes referred to as Fermat's little theorem.
- Statement:

  "If p is prime and a is a positive integer not divisible by p, then

$$a^{p-1} \equiv 1 (\mathrm{mod}\, p)$$

- An alternative form of Fermat's theorem is also useful: If p is prime and a is a positive integer, then

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

Note that the first form of the theorem requires that a be relatively prime to p, but this form does not.

Euler's Totient Function

- Euler's totient function and written $\Phi(n)$, 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.

Euler's Theorem

- Euler's theorem states that for every a and n that are relatively prime:

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

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

Group

- a set S of elements or “numbers”
  - may be finite or infinite
- with some operation ‘.’ so G=(S,.)
- 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**

Cyclic Group

- define **exponentiation** as repeated application of operator
  - example: $a^3 = a.a.a$
- and let identity be: $e=a^0$
- a group is cyclic if every element is a power of some fixed element a
  - i.e., $b = a^k$ for some a and every b in group
- a is said to be a generator of the group

Ring

- a set of “numbers”
- with two operations (addition and multiplication) which form:
- an abelian group with addition operation
- and multiplication:
  - has closure
  - is associative
  - distributive over addition: `a(b+c) = ab + ac`
- if multiplication operation is commutative, it forms a **commutative ring**
- if multiplication operation has an identity and no zero divisors, it forms an **integral domain**

Field

- a set of numbers
- with two operations which form:
  - abelian group for addition
  - abelian group for multiplication (ignoring 0)
  - ring
- have hierarchy with more axioms/laws
  - group -> ring -> field

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 0, there is an element a^{-1} in S such that $aa^{-1} = a^{-1}a = 1$

Finite (Galois) Fields

- finite fields play a key role in cryptography
- can show number of elements in a finite field **must** be a power of a prime p^n
- 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 {0,1, … , p-1} with arithmetic operations modulo prime p
- these form a finite field
  - since have multiplicative inverses
  - find inverse with Extended Euclidean algorithm

GF(7) Multiplication Example

×	0	1	2	3	4	5	6
0	0	0	0	0	0	0	0
1	0	1	2	3	4	5	6
2	0	2	4	6	1	3	5
3	0	3	6	2	5	1	4
4	0	4	1	5	2	6	3
5	0	5	3	1	6	4	2
6	0	6	5	4	3	2	1

Polynomial Arithmetic

- can compute using polynomials

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

- several alternatives available
  - ordinary polynomial arithmetic
  - poly arithmetic with coefs mod p
  - poly arithmetic with coefs mod p and polynomials mod m(x)

Ordinary Polynomial Arithmetic

- add or subtract corresponding coefficients
- multiply all terms by each other
- eg

let $f(x) = x^3 + x^2 + 2$ and $g(x) = x^2 - x + 1$

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

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

$f(x) \text{ x } g(x) = x^5 + 3x^2 - 2x + 2$

Polynomial Arithmetic with Modulo Coefficients

- when computing value of each coefficient do calculation modulo some value
  - forms a polynomial ring
- could be modulo any prime
- but we are most interested in mod 2
  - i.e. all coefficients are 0 or 1
  - e.g. let $f(x) = x^3 + x^2$ and $g(x) = x^2 + x + 1$

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

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

Polynomial Division

- can write any polynomial in the form:
  - $f(x) = q(x)\ g(x) + r(x)$
  - can interpret $r(x)$ as being a remainder
  - $r(x) = f(x) \bmod g(x)$
- if have no remainder say $g(x)$ divides $f(x)$
- if $g(x)$ has no divisors other than itself & 1 say it is **irreducible** (or prime) polynomial
- arithmetic modulo an irreducible polynomial forms a field.

$$f(x) = a_{n-1}x^{n-1} + a_{n-2}x^{n-2} + \cdots + a_1x + a_0 = \sum_{i=0}^{n-1} a_i x^i$$

- Consider the set S of all polynomials of degree n−1 or less over the field Z_p. Thus, each polynomial has the form
- where each a_i takes on a value in the set {0, 1,..., p−1}. There are a total of $\mathbf{p^n}$ different polynomials in S.
- **For p = 3 and n = 2, the 3^2 = 9 polynomials in the set are**

0	x	2x
1	x + 1	2x + 1
2	x + 2	2x + 2

- **For p = 2 and n = 3, the 2^3 = 8 the polynomials in the set are**

0	x + 1	x^2 + x
1	x^2	x^2 + x + 1
X	x^2 + 1	

- mod 2:

1 + 1 = 1−1 = 0;
1 + 0 = 1 − 0 = 1;
0 + 1 = 0 − 1 = 1.

- if $f(x)$ has no divisors other than itself & 1 it is said irreducible (or prime) polynomial, an irreducible polynomial forms a field.
- $f(x) = x^4 + 1$ over GF(2) is reducible,
  - because $x^4 + 1 = (x + 1)(x^3 + x^2 + x + 1)$
- $f(x) = x^3 + x + 1$ is irreducible residual 1.

$$
\begin{array}{r}
x^2 + x \\
x + 1 \overline{\big) x^3 \qquad + x + 1} \\
\underline{x^3 + x^2} \\
x^2 + x \\
\underline{x^2 + x} \\
1
\end{array}
$$

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

Polynomial GCD

- gcd[a(x), b(x)] is the polynomial of maximum degree that divides both a(x) and b(x).
- gcd[a(x), b(x)] = gcd[b(x), a(x)mod(b(x))]
- Euclid[$a(x)$, $b(x)$]

1. $A(x) \leftarrow a(x)$; $B(x) \leftarrow b(x)$
2. **if** $B(x) = 0$ **return** $A(x) = \gcd[a(x), b(x)]$
3. $R(x) = A(x) \bmod B(x)$
4. $A(x) \leftarrow B(x)$
5. $B(x) \leftarrow R(x)$
6. **goto** 2

Example of GCD in Z_2 or in GF(2),

Step1, gcd(A(x), B(x))

$A(x) = x^6 + x^5 + x^4 + x^3 + x^2 + 1$,

$B(x) = x^4 + x^2 + x + 1$; $D(x) = x^2 + x$;

$R(x) = x^3 + x^2 + 1$

Step 2,

$A(x) = B(x) = x^4 + x^2 + x + 1$;

$B(x) = R(x) = x^3 + x^2 + 1$,

$D(x) = x + 1$; $R(x) = 0$;

Step 3,

$A(x) = B(x) = x^3 + x^2 + 1$;

$B(x) = R(x) = 0$;

$\gcd(A(x), B(x)) = x^3 + x^2 + 1$

$$
\begin{array}{r}
x^2 + x \\
x^4 + x^2 + x + 1 \overline{\big) x^6 + x^5 + x^4 + x^3 + x^2 + x + 1} \\
\underline{x^6 \quad + x^4 + x^3 + x^2 \qquad\quad} \\
x^5 \qquad\qquad\qquad + x + 1 \\
\underline{x^5 \qquad + x^3 + x^2 + x \quad} \\
x^3 + x^2 \qquad + 1
\end{array}
$$

Find gcd[a(x), b(x)] for $a(x) = x^6 + x^5 + x^4 + x^3 + x^2 + x + 1$ and $b(x) = x^4 + x^2 + x + 1$.

$A(x) = a(x)$; $B(x) = b(x)$

$$
\begin{array}{r|l}
 & x^2 + x \\
\hline
x^4 + x^2 + x + 1 & x^6 + x^5 + x^4 + x^3 + x^2 + x + 1 \\
 & x^6 + x^4 + x^3 + x^2 \\
\hline
 & x^5 + x + 1 \\
 & x^5 + x^3 + x^2 + x \\
\hline
 & x^3 + x^2 + 1
\end{array}
$$

$R(x) = A(x) \bmod B(x) = x^3 + x^2 + 1$

$A(x) = x^4 + x^2 + x + 1$; $B(x) = x^3 + x^2 + 1$

$$
\begin{array}{r|l}
 & x + 1 \\
\hline
x^3 + x^2 + 1 & x^4 + x^2 + x + 1 \\
 & x^4 + x^3 + x \\
\hline
 & x^3 + x^2 + 1 \\
 & x^3 + x^2 + 1 \\
\hline
\end{array}
$$

$R(x) = A(x) \bmod B(x) = 0$

$\gcd[a(x), b(x)] = A(x) = x^3 + x^2 + 1$

Example GF(2^3)

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

(a) Addition

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

(b) Multiplication

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

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, called discrete Logarithms Problem). The difficulty seems to be on the same order of magnitude as that of factoring primes required for RSA.