Discrete Maths

Data and Information Management: ELEN 3015

School of Electrical and Information Engineering,
University of the Witwatersrand

Overview

Discrete maths

Prime Numbers

Greatest Common Divisor (GCD)

Relative Prime

The Euler Totient Function

Modular Arithmetic

Fermat's Little Theorem

1. Discrete Math

We will look at aspects of number theory that apply to cryptography.

Discrete mathematics is a branch of mathematics that deals with Integers only.

1. Discrete Math

1.1 Prime Numbers

Def - Prime Number: Any integer greater than one that only has 1 and itself as divisors

Prime numbers: 2, 3, 5, 7, 11, 13, 17, 19, 23, 29, 31, 37, 41, 43, 47, 53, 59, 61, 67, 71, 73, 79, 83, 89, 97, 101, 103, 107, 109, 113, . . .

Non-prime number is known as a composite

Fundamental theorem of arithmetic: every positive integer (except 1) can be represented in exactly one way as a product of one or more primes (Hardy and Wright 1979, pp. 2-3).

1.2 Greatest Common Divisor (GCD)

Largest integer d that divides a and $b \in \mathbb{Z} \rightarrow$ Greatest Common Divisor of a and b

Notation: $d = GCD(a, b)$

Example: $GCD(12, 16) = 4$

Euclidean algorithm can be used to determine GCD

1.3 Relative Prime

Def - Relative prime: When $GCD(a, b) = 1$, a and $b \in \mathbb{Z}$, then a and b are relative prime (also coprime)

In other words, they share no common factors other than 1

Neither a and b need to be prime

Example: $GCD(15, 28) = 1$, thus 15 and 28 are relative prime

1.4 The Euler Totient Function

Def - the totient $\varphi(n)$ of a positive integer n is defined to be the number of positive integers less than n that are relative prime to n.

$$\varphi(n) = \begin{cases} n-1, & \text{n prime} \\ (p-1)(q-1), & n = pq \text{ with } p \text{ and } q \text{ prime} \end{cases}$$

For first scenario, note that p (prime) has $\{1, 2, 3, \ldots, p-1\}$ as relative primes

Note that the second scenario only represents a small subset of the composite numbers.

1.5 Modular Arithmetic

Discrete maths operates only on integers ($\mathbb{Z}$)

Modular arithmetic restricts results to a maximum modulo size

Modulus means remainder after division

1.5 Modular Arithmetic

Def - Equivalence / Congruency: Two integers are equivalent under modulus n if their results mod n are equal

Example: $16 \bmod 7 = 23 \bmod 7 \rightarrow 16 \equiv 23 \bmod 7$

1.6 Properties of Modular Arithmetic

Modular arithmetic in non-negative integers forms a construct called a commutative ring with the operation $+$ and $\times$.

If every number other than 0 has an inverse under multiplication, the group is called a Galois field. Example: The integers a mod p forms a Galois field.

All rings have the properties of associativity and distributivity, commutative rings also have commutativity.

1.6 Properties of Modular Arithmetic

Example: Modulo 5 Addition

$+$	**0**	**1**	**2**	**3**	**4**
0					
1					
2					
3					
4					

1.6 Properties of Modular Arithmetic

Example: Modulo 5 Addition

+	**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

1.6 Properties of Modular Arithmetic

Additive identity $\rightarrow a + 0 = a$ for any $a \in \mathcal{F}$

Additive inverse of an element in $\mathcal{F}$:

$$a + (-a) = 0$$

Additive inverses:

1.6 Properties of Modular Arithmetic

Additive identity $\rightarrow a + 0 = a$ for any $a \in \mathcal{F}$

Additive inverse of an element in $\mathcal{F}$:

$$a + (-a) = 0$$

Additive inverses:

- $0 \times 0 \bmod 5 = 0$
- $1 \times 4 \bmod 5 = 0$
- $2 \times 3 \bmod 5 = 0$

1.6 Properties of Modular Arithmetic

Example: Modulo 5 Multiplication

$\times$	**0**	**1**	**2**	**3**	**4**
0					
1					
2					
3					
4					

1.6 Properties of Modular Arithmetic

Example: Modulo 5 Multiplication

$\times$	**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

1.6 Properties of Modular Arithmetic

Multiplicative identity $\rightarrow a \times e = a$ for any $a \in \mathcal{F}$

$e =$

1.6 Properties of Modular Arithmetic

Multiplicative identity $\rightarrow$ $a \times e = a$ for any $a \in \mathcal{F}$

$e = 1$

Multiplicative inverse of an element in $\mathcal{F}$:

$$a \times \frac{1}{a} = 1$$

Multiplicative Inverses:

1.6 Properties of Modular Arithmetic

Multiplicative identity $\rightarrow a \times e = a$ for any $a \in \mathcal{F}$

$e = 1$

Multiplicative inverse of an element in $\mathcal{F}$:

$$a \times \frac{1}{a} = 1$$

Multiplicative Inverses:

- $1 \times 1 \bmod 5 = 1$
- $2 \times 3 \bmod 5 = 1$
- $4 \times 4 \bmod 5 = 1$

1.7 Modulo Inverses

Finite field (Galois Field) $\rightarrow$ every element except 0 has multiplicative inverse

Ring $\rightarrow$ not every element might have an inverse

1.7 Modulo Inverses

Example: Multiplication Modulo 6

×	**0**	**1**	**2**	**3**	**4**	**5**
0	0	0	0	0	0	0
1	0	1	2	3	4	5
2	0	2	4	0	2	4
3	0	3	0	3	0	3
4	0	4	2	0	4	2
5	0	5	4	3	2	1

2,3 and 4 doesn't have inverses under modulo 6 multiplication
2,3 and 4 not relative prime to 6

Modulo under a prime number $\rightarrow$ Field (Galois Field), every nonzero element has an inverse

1.7 Modulo Inverses

Example:

$4 \times \lambda \equiv 1 \text{ mod } 7 \rightarrow 4\lambda = 7k + 1,\ k \in \mathbb{Z}$

General Problem:

$$1 = (\text{a} \times \lambda) \text{ mod } n$$

$$a^{-1} \equiv \lambda \text{ mod } n$$

For Example: $4^{-1} = 2\ (\mathcal{F} = x \mod 5)$

1.8 Fermat's Little Theorem

If p is a prime, and a is not a multiple of p:

$$a^{p-1} \equiv 1 \text{ mod p}$$

Euler's generalization:
if $GCD(a, n) = 1$:

$$a^{\varphi(n)} \text{ mod n} = 1$$

To compute inverse x:

$$x = a^{\varphi(n)-1} \mod n$$

(Can also use Euclid's algorithm)

1.9 Properties of Modular Arithmetic

Associativity	[a + (b + c)]mod n = [(a + b) + c] mod n [a × (b × c)]mod n = [(a × b) × c] mod n
Commutativity	(a + b) mod n = (b + a) mod n (a × b) mod n = (b × a) mod n
Distributivity	(a × (b + c)) mod n = ((a × b) + (a × c)) mod n
Identities	(a + 0) mod n = (0 + a) mod n = a (a × 1) mod n = (1 × a) mod n = a
Inverses	(a + (-a)) mod n = 0 (a × a^{-1}) mod n = 1
Reducibility	(a + b) mod n = ((a mod n) + (b mod n)) mod n
	(a × b) mod n = ((a mod n) × (b mod n)) mod n

1.10 Euclidean Algorithm

Not in the notes!

For any pair of positive integers a and b, we may find $\gcd(a, b)$ by repeated use of division to produce a decreasing sequence of integers $r_1 > r_2 > \cdots$ as follows.

$$
\begin{aligned}
a &= bq_1 + r_1 && 0 < r_1 < b,\\
b &= r_1 q_2 + r_2 && 0 < r_2 < r_1,\\
r_1 &= r_2 q_3 + r_3 && 0 < r_3 < r_2,\\
&\vdots && \vdots\\
r_{k-3} &= r_{k-2} q_{k-1} + r_{k-1} && 0 < r_{k-1} < r_{k-2},\\
r_{k-2} &= r_{k-1} q_k + r_k && 0 < r_k < r_{k-1},\\
r_{k-1} &= r_k q_{k+1} + 0
\end{aligned}
$$

1.11 Extended Euclidean Algorithm

Not in the notes!

For any nonzero integers a and b, there exist integers s and t such that $\gcd(a, b) = as + bt$. Moreover, $\gcd(a, b)$ is the smallest positive integer of the form $as + bt$.

Extended Euclidean Algorithm

$$r_i = r_{i-2} - \left\lfloor \frac{r_{i-2}}{r_{i-1}} \right\rfloor \cdot r_{i-1}$$

1.11 Extended Euclidean Algorithm

Example: GCD(120,23)

Step	Quotient	Remainder	Expression
1		120	$120 = 120 \times 1 + 23 \times 0$
2		23	$23 = 120 \times 0 + 23 \times 1$
3	5	5	$5 = (120 \times 1 + 23 \times 0) - (120 \times 0 + 23 \times 1) \times 5$ $5 = 120 \times 1 + 23 \times -5$

1.11 Extended Euclidean Algorithm

Example: GCD(120,23)

Step	Quotient	Remainder	Expression
1		120	$120 = 120 \times 1 + 23 \times 0$
2		23	$23 = 120 \times 0 + 23 \times 1$
3	5	5	$5 = (120 \times 1 + 23 \times 0)$ - $(120 \times 0 + 23 \times 1) \times 5$ $5 = 120 \times 1 + 23 \times$ -5
4	4	3	$3 = 23$ - 5×4 $3 = (120 \times 0 + 23 \times 1)$ -4(120 -5 $\times$ 23) $3 = 120 \times$ -4 $+ 23 \times 21$
5	1	2	$2 = 5$ - 3×1 $2 = (120 \times 1 + 23 \times$ -5) - $(120 \times$ -4 $+ 23 \times 21)$ $2 = 120 \times 5$ - 23×26
6	1	1	$1 = 3$ - 2×1 $1 = (120 \times$ -4 $+ 23 \times 21)$ - $(120 \times 5$ - $23 \times 26)$ $1 = 120 \times$ -9 $+ 23 \times 47$
7	2	0	

1.11 Extended Euclidean Algorithm

Extended Euclidean Algorithm can be used to calculate the multiplicative inverse of a number in a ring (if they exist)

From example: $1 = 120 \times -9 + 23 \times 46$

Over the ring mod 120, 23 and 46 are multiplicative inverses of each other

Summary

Discrete maths

Prime Numbers

Greatest Common Divisor (GCD)

Relative Prime

The Euler Totient Function

Modular Arithmetic

Fermat's Little Theorem

Euclidean Algorithm and Extended Euclidean Algorithm