

# Lecture 1: Some Discrete Mathematics

INB355/INN355

Faculty of Science and Technology  
Queensland University of Technology

Semester 1, 2010

## Motivation

- ▶ Cryptology makes heavy use of mathematics, computer science and engineering.
- ▶ Mostly the mathematics is *discrete mathematics* because cryptology deals with finite objects such as alphabets and blocks of characters.
- ▶ Algorithms and complexity theory are important building blocks.
- ▶ Useful aspects from engineering include tamperproofing and electromagnetic measurements as well as implementation constraints.

# Outline

## Basic Number Theory

- Primes and Factorisation

- GCD and the Euclidean Algorithm

## Integer computation

- Modular arithmetic and Euler's  $\phi$  function

- Exponentiation

- Inverses

- Solving modular equations

## Boolean Functions

- Truth Tables

- Boolean operations

# Factorisation

Let  $\mathbb{Z}$  denote the set of integers.

For  $a$  and  $b$  in  $\mathbb{Z}$ , we say that  $a$  divides  $b$  (or  $a$  is a factor of  $b$ ) if there exists  $k$  in  $\mathbb{Z}$  such that  $ak = b$ .

## Example

6 divides 18 (or  $6|18$ ), 6 does not divide 19

An integer  $p > 1$  is said to be a prime number if its only positive divisors are 1 and  $p$ .

## Example

5 is prime since  $5 = 5 \times 1$

6 is not prime since  $6 = 6 \times 1 = 3 \times 2$

## Brute force algorithm for showing $p$ is prime

1. List all primes  $< \sqrt{p}$ , say  $p_1, \dots, p_r$ .
2. Show  $p_i$  is not a factor of  $p$  for  $i = 1, \dots, r$ .

Hence  $p$  is prime.

### Example

Show  $p = 29$  is prime.

All primes  $< \sqrt{29} = 2, 3, 5$

$2|29$  ? no,  $3|29$  ? no,  $5|29$  ? no

Hence  $p = 29$  is prime.

## Basic Properties of Factors

1. If  $a$  divides  $b$  and  $a$  divides  $c$ , then  $a$  divides  $b + c$ .

### Example

$$6|18 \text{ and } 6|24 \rightarrow 6|42$$

2. If  $p$  is a prime and  $p$  divides  $ab$ , then  $p$  divides  $a$  or  $b$ .

### Example

$$7|42 \rightarrow 7|3 \text{ or } 7|14$$

## Division Algorithm

For  $a$  and  $b$  in  $\mathbb{Z}$ ,  $a > b$ , there exists  $q$  and  $r$  in  $\mathbb{Z}$  such that  $a = bq + r$  where  $0 < r < b$ .

### Example

$$17 = 5 \times 3 + 2$$

## Greatest common divisor (GCD)

$d$  is the GCD of  $a$  and  $b$  (written  $\gcd(a, b) = d$ ) provided

1.  $d$  divides  $a$  and  $b$ ,
2. if  $c$  divides  $a$  and  $b$  then  $c$  divides  $d$ ,
3.  $d > 0$ .

### Example

$$\gcd(6, 15) = 3, \gcd(16, 20) = 4$$

$a$  and  $b$  are **relatively prime** if  $\gcd(a, b) = 1$ .

### Example

$$\gcd(5, 8) = 1, \gcd(9, 10) = 1$$

## Euclidean algorithm

One can find  $d = \gcd(a, b)$ .

Let  $q_i$  be the quotient and  $r_i$  be the remainder in the following.

$$a = bq_1 + r_1, \text{ for } 0 < r_1 < b$$

$$b = r_1q_2 + r_2, \text{ for } 0 < r_2 < r_1$$

$$r_1 = r_2q_3 + r_3, \text{ for } 0 < r_3 < r_2$$

$$\vdots$$

$$r_{k-2} = r_{k-1}q_k + r_k, \text{ for } 0 < r_k < r_{k-1}$$

$$r_{k-1} = r_kq_{k+1}, \text{ where } r_{k+1} = 0$$

Then  $d = r_k = \gcd(a, b)$ .

**Input:**  $a, b$

**Output:**  $\gcd(a, b)$

$r_{-1} \leftarrow a;$

$r_0 \leftarrow b;$

$k \leftarrow 0;$

**while**  $r_k \neq 0$  **do**

$q_k \leftarrow \lfloor \frac{r_{k-1}}{r_k} \rfloor;$   
     $r_{k+1} \leftarrow r_{k-1} - q_k r_k;$   
     $k \leftarrow k + 1;$

**end**

$k \leftarrow k - 1;$

**return**  $r_k$

**Algorithm 1:** Euclidean algorithm

## Example

Find  $\gcd(10175, 2277)$

$$10175 = 4 \times 2277 + 1067$$

$$2277 = 2 \times 1067 + 143$$

$$1067 = 7 \times 143 + 66$$

$$143 = 2 \times 66 + 11$$

$$66 = 6 \times 11$$

$$\gcd(2277, 10175) = 11$$

## Back substitution

By back substitution of the Euclidean algorithm we can find integers  $x$  and  $y$  where

$$ax + by = d = r_k.$$

Starting with the penultimate line in the algorithm,

$r_{k-2} = r_{k-1}q_k + r_k$ , we can compute

$$r_k = r_{k-2} - r_{k-1}q_k.$$

Then we replace  $r_{k-1}$  in this equation from the next line up,

$r_{k-1} = r_{k-3} - r_{k-2}q_{k-1}$  to get

$$\begin{aligned} r_k &= r_{k-2} - (r_{k-3} - r_{k-2}q_{k-1})q_k \\ &= r_{k-2}(1 + q_{k-1}q_k) - r_{k-3}q_k \end{aligned}$$

- ▶ Now we can use this equation to replace  $r_{k-2}$  from the line before that, and continue in the same way.
- ▶ Finally replacing  $r_1$  by  $r_1 = a - bq_1$  from the first line gives us  $r_k$  in terms of a multiple of  $a$  and a multiple of  $b$ .
- ▶ We will be particularly interested in the case where  $r_k = d = 1$ .

## Example

Determine integers  $x, y$  such that  $11 = 2277x + 10175y$  (back substitution of Euclidean algorithm):

$$\begin{aligned}11 &= 143 - 2 \times 66 \\ &= 143 - 2(1067 - 7 \times 143) \\ &= 15 \times 143 - 2 \times 1067 \\ &= 15(2277 - 2 \times 1067) - 2 \times 1067 \\ &= 15 \times 2277 - 32 \times 1067 \\ &= 15 \times 2277 - 32(10175 - 4 \times 2277) \\ &= 143 \times 2277 - 32 \times 10175\end{aligned}$$

$$\rightarrow x = 143, y = -32$$

## Properties of GCD

1.  $\gcd(a, b) = 1$  iff there exists  $x$  and  $y$  with  $ax + by = 1$ .
2. If  $a$  divides  $bc$  and  $\gcd(a, b) = 1$  then  $a$  divides  $c$ .
3.  $ax + by = k$  has integer solutions for  $x$  and  $y$  iff  $d$  divides  $k$  where  $d = \gcd(a, b)$ .
4. If  $d = \gcd(a, b)$  then  $\gcd(a_0, b_0) = 1$  where  $da_0 = a$  and  $db_0 = b$ .

# Modular arithmetic

## Definition

$b$  is a residue of  $a$  modulo  $n$  if  $a - b = kn$  for some integer  $k$ .

$$a \equiv b \pmod{n} \iff a - b = kn.$$

## Example

$$29 \equiv 5 \pmod{12} \quad \text{since} \quad 29 - 5 = 2 \times 12$$

$$-9 \equiv 5 \pmod{7} \quad \text{since} \quad -9 - 5 = -2 \times 7$$

and vice versa

## Elementary properties

Given  $a \equiv b \pmod{n}$  and  $c \equiv d \pmod{n}$ , then

1.  $a + c \equiv (b + d) \pmod{n}$ ,
2.  $ac \equiv bd \pmod{n}$
3.  $ka \equiv kb \pmod{n}$ .

In particular we can always reduce the inputs modulo  $n$  *before* performing multiplication or addition.

## Modular arithmetic and cryptography

Some benefits of using modular arithmetic in cryptographic systems:

- ▶ restriction to a fixed set of integers  $[0, n - 1]$  allows mapping from message spaces;
- ▶ allows exact recovery of input values (in contrast to using floating point arithmetic);
- ▶ provide a source of intractable problems, for example computing logarithms.

## Residue class

### Definition

$\{r_0, r_1, \dots, r_{n-1}\}$  is called a complete set of residues  $(\text{mod } n)$  if, for every integer  $a$ ,  $a \equiv r_i \pmod{n}$  for exactly one  $r_i$ .

The numbers  $\mathbb{Z}_n = \{0, 1, \dots, n-1\}$  form a complete set of residues  $(\text{mod } n)$  since

$$a = qn + r \text{ for } 0 \leq r \leq n-1$$

Usually the set  $\mathbb{Z}_n = \{0, 1, \dots, n-1\}$  is used.

## Reduced set of residues

### Definition

For a positive integer  $n$ , the Euler function  $\phi(n)$  denotes the number of positive integers less than  $n$  and relatively prime to  $n$ .

### Example

$\phi(10) = 4$  since 1,3,7,9 are each relatively prime to 10.

The set of positive integers less than  $n$  and relatively prime to  $n$  form the reduced residue class  $\mathbb{Z}_n^*$ .

$$\mathbb{Z}_{10}^* = \{1, 3, 7, 9\}$$

## Notation: $a \bmod n$

We write

$$a \bmod n$$

to denote the unique value  $a'$  in the reduced set of residues  $\{0, 1, \dots, n-1\}$  with

$$a' \equiv a \pmod{n}.$$

In other words,  $a \bmod n$  is the remainder after dividing  $a$  by  $n$ .

### Example

$$5 \bmod 2 = 1$$

$$17 \bmod 11 = 6$$

## Properties of $\phi(n)$

1.  $\phi(p) = p - 1$  for  $p$  prime.
2.  $\phi(pq) = (p - 1)(q - 1)$  for  $p$  and  $q$  distinct primes.
3. Let  $n = p_1^{e_1} \dots p_t^{e_t}$  where  $p_i$  are distinct primes. Then

$$\phi(n) = \prod_{i=1}^t p_i^{e_i-1} (p_i - 1)$$

where  $\prod$  represents the product.

### Example

$$\phi(15) = 2 \times 4 = 8$$

$$\phi(24) = 2^2(2 - 1)3^0(3 - 1) = 8$$

$$\text{(where } 24 = 2^3 \times 3\text{)}$$

## Two important theorems

### Theorem (Fermat)

*Let  $p$  be a prime. Then*

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

*for all integers  $a$  with  $1 < a < p - 1$ .*

### Theorem (Euler)

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

*if  $\gcd(a, n) = 1$ .*

When  $p$  is prime then  $\phi(p) = p - 1$  so Fermat's theorem is a special case of Euler's theorem.

## Binary representation

Let  $n$  be an integer where  $0 < n < 2^k$ . Then we can express  $n$  as

$$n = e_0 + e_1 2 + e_2 4 + \dots + e_{k-1} 2^{k-1}$$

where

- ▶  $e_i$  are binary digits,
- ▶  $e_0$  is least significant bit,  
and
- ▶  $e_{k-1}$  is most significant bit.

We can identify  $n$  with a binary  $k$ -vector  $(e_{k-1}, \dots, e_0)$ .

## Example

$$157 = 1 \times 1 + 0 \times 2 + 1 \times 4 + 1 \times 8 + 1 \times 16 + 0 \times 32 + 0 \times 64 + 1 \times 128.$$

- ▶ Binary representation of 157 is (10011101).
- ▶ Note that in the binary vector we sets the right-most bit as the lowest-order (least significant) bit.

## Fast exponentiation

- ▶ One common problem in many cryptographic systems is computing  $m^e \bmod n$  fast for large  $e$  and  $n$ .
- ▶ Technique:  
Write  $e$  in index 2 representation.

$$e = e_0 2^0 + e_1 2^1 + \dots + e_k 2^k$$

where  $e_i$  are binary digits

- ▶ The basic idea behind fast exponentiation is the *square and multiply* algorithm. There are a few variants and we just look at one.

## Square and multiply algorithm

$$m^e = m^{e_0} (m^2)^{e_1} (m^4)^{e_2} \dots (m^{2^k})^{e_k}$$

**Input:**  $m, n, e = e_k e_{k-1} \dots e_1 e_0$

**Output:**  $m^e \bmod n$

$z \leftarrow 1;$

**for**  $i = 0$  to  $k$  **do**

**if**  $e_i = 1$  **then**

$z \leftarrow z * m \bmod n;$

**end**

$m \leftarrow m^2 \bmod n;$

**end**

**return**  $z$

**Algorithm 2:** Square and multiply algorithm

## Example

Evaluate  $17^{93} \bmod 23$

$$e = 93 = 1 \times 2^0 + 0 \times 2^1 + 1 \times 2^2 + 1 \times 2^3 + 1 \times 2^4 + 0 \times 2^5 + 1 \times 2^6$$

$$\begin{aligned} 17^{93} \bmod 23 &= (((((((17^1)^2 17^0)^2 17^1)^2 17^1)^2 17^1)^2 17^0)^2 17^1 \\ &= (((17^4 17)^2 17)^2 17)^4 17 \\ &= 21 \end{aligned}$$

## Computing inverses modulo $n$

### Theorem

Let  $0 < a < n$ . Then there exists  $x$  such that  $ax \equiv 1 \pmod{n}$  iff  $\gcd(a, n) = 1$ .

The  $x$  from the above theorem is called the inverse of  $a$  and is written  $a^{-1} \pmod{n}$ .

## Example

Take  $n = 10$ .

$$3 \times 7 \equiv 1 \pmod{10} \quad \text{so} \quad 3^{-1} = 7 \text{ and } 7^{-1} = 3$$

$$9 \times 9 \equiv 1 \pmod{10} \quad \text{so} \quad 9^{-1} = 9$$

$$1 \times 1 \equiv 1 \pmod{10} \quad \text{so} \quad 1^{-1} = 1$$

- ▶ To find the inverse of  $a$  we mention three methods. The third one (Euclidean algorithm) is by far the most efficient.
- ▶ Remember that we want to solve for  $x$ , given  $a$ :

$$ax \equiv 1 \pmod{n}.$$

## Modular inverses method 1: Brute force

Compute  $a, a^2, \dots \pmod{n}$  until we find  $a^r \equiv 1 \pmod{n}$ . Then

$$\begin{aligned} a \cdot a^{r-1} &\equiv 1 \pmod{n} \\ x &= a^{r-1} \end{aligned}$$

This method is computationally infeasible when  $n$  is moderately large (say 100 bits in length).

## Modular inverses method 2: Euler's theorem

If  $\phi(n)$  is known then

$$a^{\phi(n)} \equiv 1 \pmod{n} \Rightarrow x = a^{\phi(n)-1}.$$

### Example

Find  $29^{-1} \pmod{181}$ .

$$\begin{aligned}x &\equiv a^{\phi(n)-1} \pmod{181} \\ &\equiv 29^{180-1} \pmod{181} \\ &\equiv 25 \pmod{181}\end{aligned}$$

## Modular inverses method 3: Euclidean algorithm

Since  $\gcd(a, n) = 1$  we can find  $ax + ny = 1$  for integers  $x$  and  $y$  by Euclidean algorithm. Therefore:

$$\begin{aligned}ax &= 1 + yn \\ax &\equiv 1 \pmod{n}\end{aligned}$$

### Example

Find  $29^{-1} \pmod{181}$ . Use Euclidean algorithm to obtain  $ax + ny = 1$ .

$$\begin{aligned}29 \times 25 + 181 \times (-4) &= 1 \\x &\equiv 25 \pmod{181}\end{aligned}$$

## Computing $2 \times 2$ matrix inverses (mod $n$ )

Let  $A = \begin{bmatrix} a & b \\ c & d \end{bmatrix} \pmod{n}$  and  $I = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$  (identity matrix).

### Theorem

There exists  $X$  such that  $AX \equiv I \pmod{n}$  iff  $|A| \neq 0$  and  $\gcd(|A|, n) = 1$  where  $|A| = ad - bc \pmod{n}$  is the determinant of  $A$ . If  $X$  exists then

$$X = A^{-1} = |A|^{-1} \begin{bmatrix} d & -b \\ -c & a \end{bmatrix} \pmod{n}$$

If  $A^{-1}$  does not exist, then we say  $A$  is *singular*. Otherwise  $A$  is *non-singular*.

## Example

Let

$$A = \begin{bmatrix} 26 & 24 \\ 19 & 7 \end{bmatrix} \pmod{27}$$

Find  $A^{-1}$ . Note that some steps are omitted in the following calculation.

$$\begin{aligned} A^{-1} &= (26 \times 7 - 24 \times 19)^{-1} \begin{bmatrix} 7 & -24 \\ -19 & 26 \end{bmatrix} \pmod{27} \\ &= (20 - 24)^{-1} \begin{bmatrix} 7 & 3 \\ 8 & 26 \end{bmatrix} \pmod{27} \\ &= 20 \begin{bmatrix} 7 & 3 \\ 8 & 26 \end{bmatrix} \pmod{27} \\ &= \begin{bmatrix} 5 & 6 \\ 25 & 7 \end{bmatrix} \pmod{27} \end{aligned}$$

## Solving a set of simultaneous equations

### Example

$$\begin{aligned} 21 &\equiv 8a + b \pmod{27} \\ 16 &\equiv 19a + b \pmod{27} \end{aligned}$$

$$\begin{pmatrix} 21 \\ 16 \end{pmatrix} \equiv \begin{pmatrix} 8 & 1 \\ 19 & 1 \end{pmatrix} \begin{pmatrix} a \\ b \end{pmatrix} \pmod{27}$$

$$\begin{aligned} \begin{pmatrix} a \\ b \end{pmatrix} &\equiv \begin{pmatrix} 8 & 1 \\ 19 & 1 \end{pmatrix}^{-1} \begin{pmatrix} 21 \\ 16 \end{pmatrix} \pmod{27} \\ &\equiv \begin{pmatrix} 22 & 5 \\ 14 & 14 \end{pmatrix} \begin{pmatrix} 21 \\ 16 \end{pmatrix} \pmod{27} \\ &\equiv \begin{pmatrix} 2 \\ 5 \end{pmatrix} \pmod{27} \end{aligned}$$

## Solving a set of simultaneous equations

### Example

$$21 \equiv 8a + b \pmod{27}$$

$$16 \equiv 19a + b \pmod{27}$$

Alternative solution. Subtract second equation from first.

$$5 = -11a \pmod{27}$$

$$5 = 16a \pmod{27}$$

$$a = 5 \times 16^{-1} \pmod{27}$$

$$a = 5 \times 22 \pmod{27}$$

$$a = 110 \pmod{27} = 2$$

Then solve for  $b$  using either equation.

## Chinese remainder theorem

### Theorem

*Let  $d_1, d_2, \dots, d_r$  be pairwise relatively prime and  $n = d_1 d_2 \dots d_r$ . Given any integers  $c_i$  there exists a unique integer  $x$  with  $0 \leq x < n$  such that*

$$x \equiv c_1 \pmod{d_1}$$

$$x \equiv c_2 \pmod{d_2}$$

$$\vdots$$

$$x \equiv c_r \pmod{d_r}$$

In fact  $x \equiv \sum (\frac{n}{d_i}) y_i c_i \pmod{n}$  where  $y_i \equiv (\frac{n}{d_i})^{-1} \pmod{d_i}$ .

## Example

$$\begin{aligned} \text{Solve } x &\equiv 5 \pmod{6} \\ x &\equiv 33 \pmod{35} \end{aligned}$$

Since 6 and 35 are relatively prime we can use CRT. Set  $n = 6 \times 35 = 210$ .

$$\begin{array}{ll} \frac{210}{6}y_1 &\equiv 1 \pmod{6} & \frac{210}{35}y_2 &\equiv 1 \pmod{35} \\ 35y_1 &\equiv 1 \pmod{6} & 6y_2 &\equiv 1 \pmod{35} \\ y_1 &\equiv 5 \pmod{6} & y_2 &\equiv 6 \pmod{35} \end{array}$$

$$\begin{aligned} x &\equiv \sum \left(\frac{n}{d_i}\right) y_i c_i \pmod{n} \\ &\equiv (35 \times 5 \times 5) + (6 \times 6 \times 33) \pmod{210} \\ &\equiv 175 \times 5 + 36 \times 33 \pmod{210} \\ &\equiv 173 \pmod{210} \end{aligned}$$

## Truth tables

- ▶ A binary variable  $x$  takes the values of 0 or 1. Let  $x_1, \dots, x_n$  be  $n$  binary variables.
- ▶ A binary variable  $z$  is said to be a Boolean function of these  $n$  input variables if  $z = f(x_1, \dots, x_n)$ . This can be represented by a table.
- ▶ Each row in the table defines one possible tuple of the  $n$  input variables plus the associated output value for that tuple.

- ▶ Number of rows in table: For  $n$  input variables there are  $2^n$  possible values, therefore the table has  $2^n$  rows.
- ▶ Number of columns in table: There is one column per input variable plus one column for the output values, therefore the table has  $n + 1$  columns.
- ▶ Such a table is called a *truth table*.

## Example

$x_1$	$x_2$	$x_3$	$z$
0	0	0	0
1	0	0	1
0	1	0	0
0	0	1	0
1	1	0	0
1	0	1	1
0	1	1	1
1	1	1	1

We shall describe algebraic operations to represent basic Boolean functions.

## Exclusive OR (XOR)

Write  $z = x_1 \oplus x_2$

Truth table

$x_1$	$x_2$	$z$
1	1	0
1	0	1
0	1	1
0	0	0

This is the operation of addition (mod 2).

## Logical AND

Write  $z = x_1 \wedge x_2$

Truth table

$x_1$	$x_2$	$z$
1	1	1
1	0	0
0	1	0
0	0	0

This is the operation of multiplication (mod 2).

# Negation

## Truth table

$x$	$\neg x$
1	0
0	1

We can also write  $\neg x = x \wedge 1$

## Logical OR operation

Write  $z = x_1 \vee x_2$

Truth table

$x_1$	$x_2$	$z$
1	1	1
1	0	1
0	1	1
0	0	0

We can also express this as  $z = x_1 \oplus x_2 \oplus (x_1 \wedge x_2)$