CS 441 Discrete Mathematics for CS
Lecture 16

Congruencies

Milos Hauskrecht
milos@cs.pitt.edu
5329 Sennott Square

Modular arithmetic

- In computer science we often care about the remainder of an integer when it is divided by some positive integer.

Problem: Assume that it is a midnight. What is the time on the 24 hour clock after 50 hours?

Answer: ?

Modular arithmetic

- In computer science we often care about the remainder of an integer when it is divided by some positive integer.

Problem: Assume that it is a midnight. What is the time on the 24 hour clock after 50 hours?

Answer: the result is 2am

How did we arrive to the result:

- Divide 50 with 24. The reminder is the time on the 24 hour clock.
  - 50= 2*24 + 2
  - so the result is 2am.

Congruency

Definition: If a and b are integers and m is a positive integer, then **a is congruent to b modulo n** if m divides a-b. We use the notation **a ≡ b (mod m)** to denote the congruency. If a and b are not congruent we write **a ≠ b (mod m).**

Example:

- Determine if 17 is congruent to 5 modulo 6?

Congruency

Definition: If a and b are integers and m is a positive integer, then **a is congruent to b modulo n** if m divides a-b. We use the notation **a ≡ b (mod m)** to denote the congruency. If a and b are not congruent we write a ≠ b (mod m).

Example:

- Determine if 17 is congruent to 5 modulo 6?
- 17 - 5=12,
- 6 divides 12
- so 17 is congruent to 5 modulo 6.

Congruency

Theorem. If a and b are integers and m a positive integer. Then a ≡ b (mod m) if and only if (a mod m) = (b mod m).

Example:

- Determine if 17 is congruent to 5 modulo 6?
- 17 mod 6 = …

Congruency

Theorem. If a and b are integers and m a positive integer. Then $a \equiv b \pmod{m}$ if and only if (a mod m) = (b mod m).

Example:

- Determine if 17 is congruent to 5 modulo 6?
- 17 mod 6 = 5
- 5 mod 6 = …

Congruency

Theorem. If a and b are integers and m a positive integer. Then $a \equiv b \pmod{m}$ if and only if (a mod m) = (b mod m).

Example:

- Determine if 17 is congruent to 5 modulo 6?
- 17 mod 6 = **5**
- 5 mod 6 = **5**
- Thus 17 is congruent to 5 modulo 6.

Congruencies: properties

Theorem 1. Let m be a positive integer. The integers a and b are congruent modulo m if and only if there exists an integer k such that $a=b+mk$.

Theorem2. Let m be a positive integer. If $a \equiv b \pmod{m}$ and $c \equiv d \pmod{m}$ then:

$$a+c \equiv b+d \pmod{m} \text{ and } ac \equiv bd \pmod{m}.$$

Modular arithmetic in CS

Modular arithmetic and congruencies are used in CS:

- **Pseudorandom number generators**
  - Generate a sequence of random numbers from some interval
- **Hash functions**
  - identify how to map information that would need to a large sparse table into a small compact table
- **Cryptology**
  - Prevent other people from reading the transmitted messages

Pseudorandom number generators

- Any randomness in the program is implemented using random number generators that generate a sequence of random numbers from some interval
  - The chance of picking any number in the interval is uniform
- **Pseudorandom number generators**: use a simple formula to define the sequence:
  - The sequence looks like it was generated randomly
  - The next element in the sequence is a deterministic function of the previous element.
  - Typically based on the modulo operation.

Next: the Linear congruential method

Pseudorandom number generators

Linear congruential method

- We choose 4 numbers:
  - the modulus m,
  - multiplier a,
  - increment c, and
  - seed x_0,

  such that $2 =< a < m$, $0 =< c < m$, $0 =< x_0 < m$.
- We generate a sequence of numbers $x_1, x_2\ x_3 \ldots x_n \ldots$ such that $0 =< x_n < m$ for all *n* by successively using the congruence:
  - $x_{n+1} = a(x_n + c) \bmod m$

Pseudorandom number generators

Linear congruential method:

- $x_{n+1} = (a\ x_n + c) \bmod m$

Example:

- Assume : m=9,a=7,c=4, $x_0 = 3$

- x_1= 7*3+4 mod 9=25 mod 9 =7
- x_2 = 53 mod 9 = 8
- x_3 =

Pseudorandom number generators

Linear congruential method:

- $x_{n+1} = a\ (x_n + c) \bmod m$

Example:

- Assume : m=9,a=7,c=4, $x_0 = 3$

- x_1= 7*3+4 mod 9=25 mod 9 =7
- x_2 = 53 mod 9 = 8
- x_3 = 60 mod 9 = 6
- x_4=

Pseudorandom number generators

Linear congruential method:

- $x_{n+1} = a\,(x_n + c) \bmod m$

Example:

- Assume : m=9,a=7,c=4, $x_0 = 3$

- $x_1 =$ 7*3+4 mod 9=25 mod 9 =7
- x_2 = 53 mod 9 = 8
- x_3 = 60 mod 9 = 6
- $x_4 =$ 46 mod 9 =1
- x_5 =

Pseudorandom number generators

Linear congruential method:

- $x_{n+1} = a\,(x_n + c) \bmod m$

Example:

- Assume : m=9,a=7,c=4, $x_0 = 3$

- $x_1 =$ 7*3+4 mod 9=25 mod 9 =7
- x_2 = 53 mod 9 = 8
- x_3 = 60 mod 9 = 6
- $x_4 =$ 46 mod 9 =1
- x_5 = 11 mod 9 =2
- x_6 =

Pseudorandom number generators

Linear congruential method:

- $x_{n+1} = a (x_n + c) \bmod m$

Example:

- Assume : m=9,a=7,c=4, $x_0 = 3$

- x_1= 7*3+4 mod 9=25 mod 9 =7
- x_2 = 53 mod 9 = 8
- x_3 = 60 mod 9 = 6
- x_4= 46 mod 9 =1
- x_5 = 11 mod 9 =2
- x_6 = 18 mod 9 =0
- ....

Cryptology

Encryption of messages.

- An idea: Shift letters in the message
  - e.g. A is shifted to D (a shift by 3)

How to represent the idea of a shift by 3?

- There are 26 letters in the alphabet. Assign each of them a number from 0,1, 2, 3, .. 25 according to the alphabetical order.

A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	Y	V	X	W	Z
0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25

- The encryption of the letter with an index p is represented as:
  - $f(p) = (p + 3) \bmod 26$

Cryptology

Encryption of messages using a shift by 3.

- The encryption of the letter with an index p is represented as:
  - f(p) = (p + 3) mod 26

Coding of letters:

A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	Y	V	X	W	Z
0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25

- **Encrypt message:**
  - **I LIKE DISCRETE MATH**
  -

Cryptology

Encryption of messages using a shift by 3.

- The encryption of the letter with an index p is represented as:
  - f(p) = (p + 3) mod 26

Coding of letters:

A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	Y	V	X	W	Z
0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25

- **Encrypt message:**
  - **I LIKE DISCRETE MATH**
  - **L**

Cryptology

Encryption of messages using a shift by 3.

- The encryption of the letter with an index p is represented as:
  - $f(p) = (p + 3) \bmod 26$

Coding of letters:

A B C D E F G H I J K L M N O P Q R S T U Y V X W Z
0 1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20 21 22 23 24 25

- **Encrypt message:**
  - **I LIKE DISCRETE MATH**
  - **L 0**

Cryptology

Encryption of messages using a shift by 3.

- The encryption of the letter with an index p is represented as:
  - $f(p) = (p + 3) \bmod 26$

Coding of letters:

A B C D E F G H I J K L M N O P Q R S T U Y V X W Z
0 1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20 21 22 23 24 25

- **Encrypt message:**
  - **I LIKE DISCRETE MATH**
  - **L 0L**

Cryptology

Encryption of messages using a shift by 3.

- The encryption of the letter with an index p is represented as:
  - f(p) = (p + 3) mod 26

Coding of letters:

A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	Y	V	X	W	Z
0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25

- **Encrypt message:**
  - **I LIKE DISCRETE MATH**
  - **L 0LN**

Cryptology

Encryption of messages using a shift by 3.

- The encryption of the letter with an index p is represented as:
  - f(p) = (p + 3) mod 26

Coding of letters:

A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	Y	V	X	W	Z
0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25

- **Encrypt message:**
  - **I LIKE DISCRETE MATH**
  - **L 0LNH GLYFUHVH PDVK.**

Cryptology

How to decode the message ?

- The encryption of the letter with an index p is represented as:
  - $f(p) = (p + 3) \bmod 26$

Coding of letters:

A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	Y	V	X	W	Z
0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25

- **What is method you would use to decode the message:**

Cryptology

How to decode the message ?

- The encryption of the letter with an index p is represented as:
  - $f(p) = (p + 3) \bmod 26$

Coding of letters:

A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	Y	V	X	W	Z
0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25

- **What is method would you use to decode the message:**
  - $\mathbf{f^{-1}(p) = (p-3) \bmod 26}$

Cryptology

How to decode the message ?

- The encryption of the letter with an index p is represented as:
  - f(p) = (p + 3) mod 26

Coding of letters:

A B C D E F G H I J K L M N O P Q R S T U Y V X W Z
0 1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20 21 22 23 24 25

- **What is method would you use to decode the message:**
  - **$f^{-1}(p)$ = (p-3) mod 26**

– **L 0LNH GLYFUHVH PDVK**

–

Cryptology

How to decode the message ?

- The encryption of the letter with an index p is represented as:
  - f(p) = (p + 3) mod 26

Coding of letters:

A B C D E F G H I J K L M N O P Q R S T U Y V X W Z
0 1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20 21 22 23 24 25

- **What is method would you use to decode the message:**
  - **$f^{-1}(p)$ = (p-3) mod 26**

– **L 0LNH GLYFUHVH PDVK**

– **I**

Cryptology

How to decode the message ?

- The encryption of the letter with an index p is represented as:
  - $f(p) = (p + 3) \bmod 26$

Coding of letters:

A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	Y	V	X	W	Z
0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25

- **What is method would you use to decode the message:**
  - $f^{-1}(p) = (p-3) \bmod 26$

– **L 0LNH GLYFUHVH PDVK**

– **I L**

Cryptology

How to decode the message ?

- The encryption of the letter with an index p is represented as:
  - $f(p) = (p + 3) \bmod 26$

Coding of letters:

A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	Y	V	X	W	Z
0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25

- **What is method would you use to decode the message:**
  - $f^{-1}(p) = (p-3) \bmod 26$

– **L 0LNH GLYFUHVH PDVK**

– **I LIKE DISCRETE MATH**