CS 441 Discrete Mathematics for CS
Lecture 13

Integers and division

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

Integers and division

- **Number theory** is a branch of mathematics that explores integers and their properties.
- **Integers:**
  - **Z integers {…, -2,-1, 0, 1, 2, …}**
  - **Z^+ positive integers {1, 2, …}**

- Number theory has many applications within computer science, including:
  - Storage and organization of data
  - Encryption
  - Error correcting codes
  - Random numbers generators

Division

Definition: Assume 2 integers a and b, such that a =/ 0 (a is not equal 0). We say that **a divides b** if there is an integer c such that b = ac. If a divides b we say that **a is a *factor* of b** and that **b is *multiple* of a**.

- The fact that a divides b is denoted as **a | b.**

Examples:

- 4 | 24 True or False ? **True**
  - 4 is a factor of 24
  - 24 is a multiple of 4
- 3 | 7 True or False ? **False**

Primes

Definition: A positive integer p that greater than 1 and that is divisible only by 1 and by itself (p) is called **a prime**.

Examples: 2, 3, 5, 7, …

1 | 2 and 2 | 2, 1 |3 and 3 | 3, etc

The Fundamental theorem of Arithmetic

Fundamental theorem of Arithmetic:

- Any positive integer greater than 1 can be expressed as a product of prime numbers.

Examples:

  - 12 = 2*2*3
  - 21 = 3*7

- Process of finding out factors of the product: **factorization**.

Primes and composites

- **How to determine whether the number is a prime or a composite?**

Let n be a number. Then in order to determine whether it is **a prime** we can test:

- **Approach 1:** if any number $x < n$ divides it. If yes it is a composite. If we test all numbers $x < n$ and do not find the proper divisor then n is a prime.
- **Approach 2:** if any prime number x < n divides it. If yes it is a composite. If we test all primes $x < n$ and do not find a proper divisor then n is a prime.
- **Approach 3:** if any prime number x $< \sqrt{n}$ divides it. If yes it is a composite. If we test all primes $x < \sqrt{n}$ and do not find a proper divisor then n is a prime.

Division

Let a be an integer and d a positive integer. Then there are unique integers, q and r, with 0 <= r < d, such that

a = dq + r.

Definitions:

- a is called the **dividend**,
- d is called the **divisor**,
- q is called the **quotient** and
- r the **remainder** of the division.

Relations:

- **q = a div d , r = a mod d**

Greatest common divisor

Definition: Let a and b are integers, not both 0. Then the largest integer d such that d | a and d | b is called **the greatest common divisor** of a and b. The greatest common divisor is denoted as gcd(a,b).

Examples:

- gcd(24,36) = ?
- 12 (start with 2,3,4,6,12)
- gcd(11,23) = ?
- 2 ways: 1) Check 2,3,4,5,6 …

  2) 11 is a prime so only the multiples of it are possible
- no positive integer greater than 1 that divides both numbers

Greatest common divisor

A systematic way to find the gcd using factorization:

- Let $a=p_1^{a1}\ p_2^{a2}\ p_3^{a3} \ldots p_k^{ak}$ and $b= p_1^{b1}\ p_2^{b2}\ p_3^{b3} \ldots p_k^{bk}$
- $gcd(a,b)= p_1^{\min(a1,b1)}\ p_2^{\min(a2,b2)}\ p_3^{\min(a3,b3)} \ldots p_k^{\min(ak,bk)}$

Examples:

- gcd(24,36) = ?
- $24 = 2*2*2*3=2^{3}*3$
- $36= 2*2*3*3=2^{2}*3^{2}$
- $gcd(24,36) =2^{2}*3 =$ **12**

Least common multiple

Definition: Let a and b are two positive integers. The least common multiple of a and b is the smallest positive integer that is divisible by both a and b. The **least common multiple** is denoted as **lcm(a,b).**

Example:

- **What is lcm(12,9) =?**
- Give me a common multiple: … 12*9= 108
- **Can we find a smaller number?**
- **Yes.** Try 36. Both 12 and 9 cleanly divide 36.

Least common multiple

A systematic way to find the lcm using factorization:

- Let $a=p_1^{a1} p_2^{a2} p_3^{a3} \dots p_k^{ak}$ and $b= p_1^{b1} p_2^{b2} p_3^{b3} \dots p_k^{bk}$
- $lcm(a,b)= p_1^{\max(a1,b1)} p_2^{\max(a2,b2)} p_3^{\max(a3,b3)} \dots p_k^{\max(ak,bk)}$

Example:

- **What is lcm(12,9) =?**
- $12 = 2*2*3=2^2*3$
- $9=3*3 =3^2$
- **lcm(12,9)** $= 2^2 * 3^2 = 4 * 9 =$ **36**

Euclid algorithm

Finding the greatest common divisor requires factorization

- $a=p_1^{a1} p_2^{a2} p_3^{a3} \dots p_k^{ak}$, $b= p_1^{b1} p_2^{b2} p_3^{b3} \dots p_k^{bk}$
- $gcd(a,b)= p_1^{\min(a1,b1)} p_2^{\min(a2,b2)} p_3^{\min(a3,b3)} \dots p_k^{\min(ak,bk)}$

- Factorization can be cumbersome and time consuming since we need to find all factors of the two integers that can be very large.

- Luckily a more efficient method for computing the gcd exists:
- It is called **Euclid's algorithm**
  - the method is known from ancient times and named after Greek mathematician Euclid.

Euclid algorithm

Assume two numbers 287 and 91. We want gcd(287,91).

- First divide the larger number (287) by the smaller one (91)
- We get 281 = 3*91 +14

Euclid algorithm

Assume two numbers 287 and 91. We want gcd(287,91).

- First divide the larger number (287) by the smaller one (91)
- We get 287 = 3*91 +14

(1) Any divisor of 91 and 287 must also be a divisor of 14:

  - 287 - 3*91 = 14

- Why? [ak – cbk] =r → (a-cb)k = r → (a-cb) = r/k (must be an integer and thus k divides r]

(2) Any divisor of 91 and 14 must also be a divisor of 287

- Why? 287 = 3 b k + dk → 287 = k(3b +d) → 287 /k = (3b +d) ← 287/k must be an integer
- **But then gcd(287,91) = gcd(91,14)**

Euclid algorithm

- **We know that gcd(287,91) = gcd(91,14)**
- But the same trick can be applied again:
    - gcd(91,14)
    - 91 = 14.6 + 7
- and therefore
    - gcd(91,14)=gcd(14,7)

- And one more time:
    - gcd(14,7) = 7
    - trivial
- **The result: gcd(287,91) = gcd(91,14)=gcd(14,7) = 7**

Euclid algorithm

Example 1:

- Find the greatest common divisor of 666 & 558

- gcd(666,558) 666=1*558 + 108
  = gcd(558,108) 558=5*108 + 18
  = gcd(108,18) 108=6*18 + 0
  = **18**

Euclid algorithm

Example 2:

- Find the greatest common divisor of 286 & 503:

- gcd(503,286) — 503=1*286 + 217
  =gcd(286, 217) — 286=1*217 + 69
  =gcd(217, 69) — 217 = 3*69 + 10
  = gcd(69,10) — 69 = 6*10 + 9
  =gcd(10,9) — 10=1*9 + 1
  = gcd(9,1) =**1**

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?
- 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 b.

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

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=b (mod m) and c=d (mod m) then:

a+c = b+d (mod m) and ac=bd (mod m).

Modular arithmetic in CS

Modular arithmetic and congruencies are used in CS:

- **Pseudorandom number generators**
- **Hash functions**
- **Cryptology**

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:
  - $x_{n+1} = (ax_n + c) \bmod m$

CS 441 Discrete mathematics for CS M. Hauskrecht

Pseudorandom number generators

Linear congruential method:

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

Example:

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

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

CS 441 Discrete mathematics for CS M. Hauskrecht

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:
  - $f(p) = (p + 3) \bmod 26$

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**
  -

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:
  - $f(p) = (p + 3) \mod 26$

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:**

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:**
  - $\mathbf{f^{-1}(p) = (p-3) \bmod 26}$