CS 441 Discrete Mathematics for CS
Lecture 15

Integers and division

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

Course administration

Homework set 5 is out

- **Due on Friday, February 24 , 2006**

Course web page:

http://www.cs.pitt.edu/~milos/courses/cs441/

Division

Let a be an integer and d a positive integer. Consider the task a/d . 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) = ?

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) = ?
- Check 2,3,4,6,12 gcd(24,36) = 12
- gcd(11,23) = ?

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) =

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: …

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?**

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

Example:

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

Least common multiple

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

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

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

- 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 **Euclidean 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 287 = 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 – 3bk] = 14 → (a-3b)k = 14 → (a-3b) = 14/k (must be an integer and thus k divides 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 – 3bk] = 14 → (a-3b)k = 14 → (a-3b) = 14/k (must be an integer and thus k divides 14]

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

- Why? 287 = 3bk + dk → 287 = k(3b +d) → 287 /k = (3b +d) ← 287/k must be an integer

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

- [ak – 3bk] = 14 → (a-3b)k = 14 → (a-3b) = 14/k (must be an integer and thus k divides 14]

(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
- **<u>But then gcd(287,91) = gcd(91,14)</u>**

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 + …

Euclid algorithm

Example 1:

- Find the greatest common divisor of 666 & 558

- gcd(666,558) 666=1*558 + 108

  =

Euclid algorithm

Example 1:

- Find the greatest common divisor of 666 & 558

- gcd(666,558) 666=1*558 + 108
-

  = gcd(558,108) 558=…*108 + …

  =

Euclid algorithm

Example 1:

- Find the greatest common divisor of 666 & 558

- gcd(666,558)   666=1*558 + 108
-

  = gcd(558,108)   558=4 *108 + 18

  =

Euclid algorithm

Example 1:

- Find the greatest common divisor of 666 & 558

- gcd(666,558)   666=1*558 + 108
-

  = gcd(558,108)   558=4*108 + 18

  = gcd(108,18)   108= … *18 + …

Euclid algorithm

Example 1:

- Find the greatest common divisor of 666 & 558

- gcd(666,558)   666=1*558 + 108
-

  = gcd(558,108)   558=4*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=

Euclid algorithm

Example 2:

- Find the greatest common divisor of 286 & 503:

- gcd(503,286) 503=1*286 + 217
  =gcd(286, 217) 286=

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 =

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 =

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 =

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**