CS 173: Discrete Structures

Eric Shaffer
Office Hour: Wed. 12-1, 2215 SC
shaffer1@illinois.edu

Announcements

Quiz Wed. Feb. 11th, end of class

- Questions?

Agenda

- Section 3.5
  - prime numbers
  - gcd, lcm
- Section 3.6
  - Euclidean algorithm
  - Number representations

Stepping into the way-back machine

- The **mod** function
  - 13 mod 3 = 1
  - -97 mod 11 = 2
  - -12 mod 5 = 3
- What is the fundamental theorem of arithmetic

$\forall n \in \mathbb{Z}$ with $n \geq 2$, n can be expressed as a unique product of primes.

Stepping into the way-back machine

- What does $a \equiv b \pmod{m}$ mean?

Stepping into the way-back machine

$a \equiv b \pmod{m}$

a,b are integers

m is a positive integer

- Definition: $a \equiv b \pmod{m}$ iff $m \mid (a-b)$
- Theorem: $a \equiv b \pmod{m}$ iff $a = b+km$

(mod) congruence identities

Suppose $a \equiv b \pmod m$ and $c \equiv d \pmod m$

Then:

$a = b + km$ and $c = d + jm$ for some $j, k \in \mathbb{Z}$

by Thm on prev. page

$a + c = b + d + km + jn$

$(a+c) = (b+d) + m(k+j)$

so

$a+c \equiv b+d \pmod m$

by Thm on prev page

Greatest Common Divisor

- Definition: Let a and b be integers (not both 0)
  - Let d be the largest integer with $d|a$ and $d|b$
  - d is called the **greatest common divisor** of a and b
  - written as **gcd(a,b)**

- Integers a and b are **relatively prime** if gcd(a,b)=1

Greatest Common Divisor

- Define gcd in terms of the prime factorizations of *a*,*b*
- Let p_n be the largest prime such that $p_n | a$ ~~and~~ or $p_n | b$

$$a = p_0^{a_0} p_1^{a_1} \cdots p_n^{a_n}$$

$$b = p_0^{b_0} p_1^{b_1} \cdots p_n^{b_n}$$

$$\gcd(a,b) = p_0^{\min(a_0,b_0)} \cdots p_n^{\min(a_n,b_n)}$$

Least Common Multiple

- Definition: Let a and b be positive integers
  - Let m be the smallest integer with $a|m$ and $b|m$
  - m is called the **least common multiple** of a and b
  - written as **lcm(a,b)**

Least Common Multiple

- Define lcm in terms of the prime factorizations of a,b

$$lcm(a,b) = p_0^{\max(a_0,b_0)} \cdots p_n^{\max(a_n,b_n)}$$

- What is lcm(a,b)gcd(a,b)? $= ab$

Euclidean Algorithm

- Oldest(?) known algorithm, known to Euclid ~300 BC
- Procedure for computing the gcd of two positive integers

Procedure: gcd(positive integer *a*, positive integer *b*)

```
x := a, y := b
while (y > 0)
begin
        r := x  mod y
        x := y
        y := r
end
```

gcd (a,b) is *x*

Euclidean Algorithm

Procedure: gcd(positive integer *a*, positive integer *b*)

x := *a*, *y* := *b*

while (*y* > 0)

begin

r := *x* mod *y*

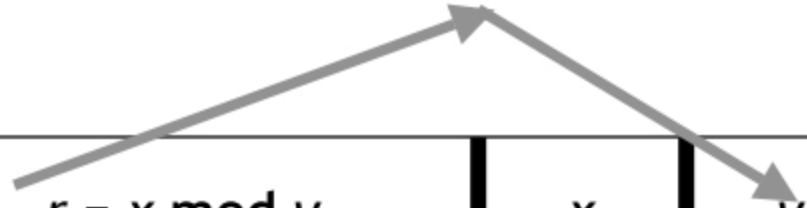
x := *y*

y := r

end

Euclidean Algorithm. Example

gcd(33,77):



Step	$r = x \bmod y$	x	y
0	–	33	77
1	33 **mod** 77 = 33	77	33
2	77 **mod** 33 = 11	33	11
3	33 **mod** 11 = 0	11	0

Euclidean Algorithm

- Oldest(?) known algorithm, known to Euclid ~300 BC
- Based on the following observation:

If a = bq +r then gcd(a,b) = gcd(b,r)
with a,b,q,r all integers

$kd = mdq + r$

$r = d(k - mq)$

so $d \mid r$

Proof

if d|a and d|b then d|(a-bq) because a=kd,b=md
so d|r since r=a-bq

Any divisor d of a and b also is a divisor of b and r
Similarly any divisor of b and r also divides a and b
So the gcd(a,b) = gcd(b,r)

Euclidean Algorithm

- Let a,b be positive integers with $a \geq b$
- Let $r_0=a$ and $r_1=b$ and successively apply the division alg.

$r_0=r_1q_1+r_2$ with $0 \leq r_2 < r_1$

$r_1=r_2q_2+r_3$ with $0 \leq r_3 < r_2$

...

$r_{n-3}=r_{n-2}q_{n-2}+r_{n-1}$ with $0 \leq r_{n-1} < r_{n-2}$

$r_{n-2}=r_{n-1}q_{n-1}+r_n$ with $0 \leq r_n < r_{n-1}$

$r_{n-1}=r_nq_n+0$

We know $r_n = \gcd(r_{n-1},r_n)=\ldots=\gcd(r_2,r_1)=\gcd(r_1,r_0)$

Euclidean Algorithm. Example

gcd(244,117):

Step	$r = x \bmod y$	x	y
0	–	244	117
1	244 **mod** 117 = 10	117	10
2	117 **mod** 10 = 7	10	7
3	10 **mod** 7 = 3	7	3
4	7 **mod** 3 = 1	3	1
5	3 **mod** 1=0	1	0

By definition ➔ 244 and 117 are rel. prime.

Representations of Integers

- Let n be an integer greater than 1
  - N can be uniquely represented in the form

$$n = a_k b^k + a_{k-1} b^{k-1} + \ldots + a_1 b^1 + a_0$$

  - This is the base b representation of n

- Name some bases….

Number Systems

EG: base-2 (***binary***) 101, 00010

base-8 (***octal***) 74, 0472

base-16 (***hexadecimal***) 12F, ABCD

Q: Compute the base 10 version of these.

Number Systems

A: base-2 (***binary***) 101, 00010

$(101)_2 = 1 \cdot 2^2 + 0 \cdot 2^1 + 1 \cdot 2^0 = 5$

$(00010)_2 = 0 \cdot (2^4+2^3+2^2+2^0) + 1 \cdot 2^1 = 2$

base-8 (***octal***) 74, 0472

$(74)_8 = 7 \cdot 8^1 + 4 \cdot 8^0 = 60$

$(0472)_8 = 4 \cdot 8^2 + 7 \cdot 8^1 + 2 \cdot 8^0 = 314$

base-16 (***hexadecimal***) 12F, ABCD

$(12F)_{16} = 1 \cdot 16^2 + 2 \cdot 16^1 + 15 \cdot 16^0 = 303$

$(ABCD)_{16} = 10 \cdot 16^3 + 11 \cdot 16^2 + 12 \cdot 16^1 + 13 \cdot 16^0 = 43981$

Number Systems

- Binary is the most natural system for bit-strings
  - hexadecimal compact way to express byte-strings
    - 1 byte = 2 hexadecimals
    - in HTML:

       Nice Color

Q: What color will this become?

Number Systems

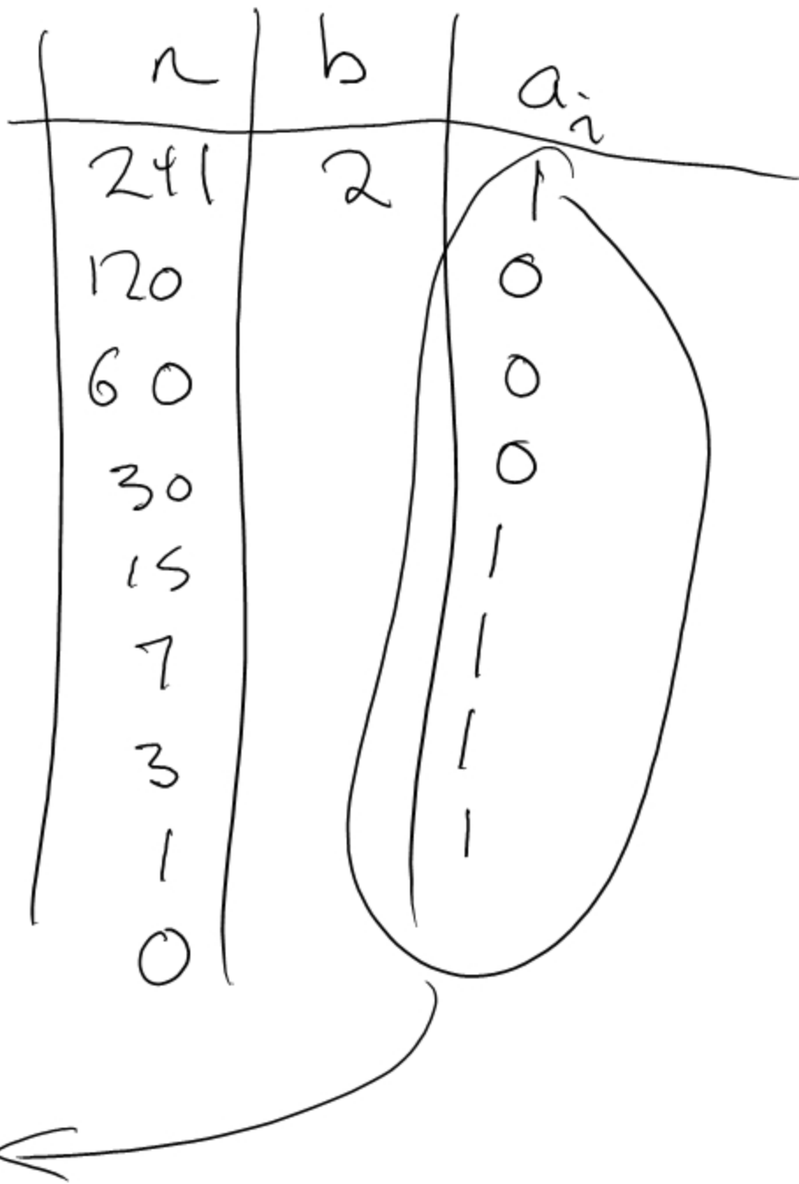
A: "**ff**00**ff**" represents the ***rgb -value***:

The first byte is for **r**edness, the second byte is for **g**reen-ness, and the last for **b**lue-ness. The HTML above specifies that 15·16 + 15 = 255 redness and blueness values, but 0·16 + 0 = 0 green-ness. Red and blue give purple, and 255 is the top brightness so this is ***bright purple***.

Number Systems
Reverse Conversion

- Conversion of integer *n* to base *b*
- Let $a_k, a_{k-1}, \ldots, a_0$ be the "digits" of the base b number

```
Procedure convert(n,b:integers)
i := 0
while (n > 0)
begin
    a_i := n mod b
    n := n ÷ b
end
```



- Convert 241 to binary

$241 = 11110001_{(2)}$

An infinite number of primes…

- Consider the formula from the proof: $k = (p_1 p_2 \ldots p_m + 1)$
- Note that k is prime ONLY IF p_m is the largest prime
  - Have we proved k will be a prime in the "real world"?

  - How can we prove whether or not k will be prime?
    - Disprove using a counter-example
    - Consider (2•3•7•11)+1= 30031

An infinite number of primes…

Some interesting facts….

- No known formula generates all primes
- No known formula generates only primes
- Some formulas generate only 1's and primes:
  - For example:

    For $n \geq 2$, set $a(n) = a(n-1) + \gcd(n, a(n-1))$

    In a paper by Rowland, Aug. 2008