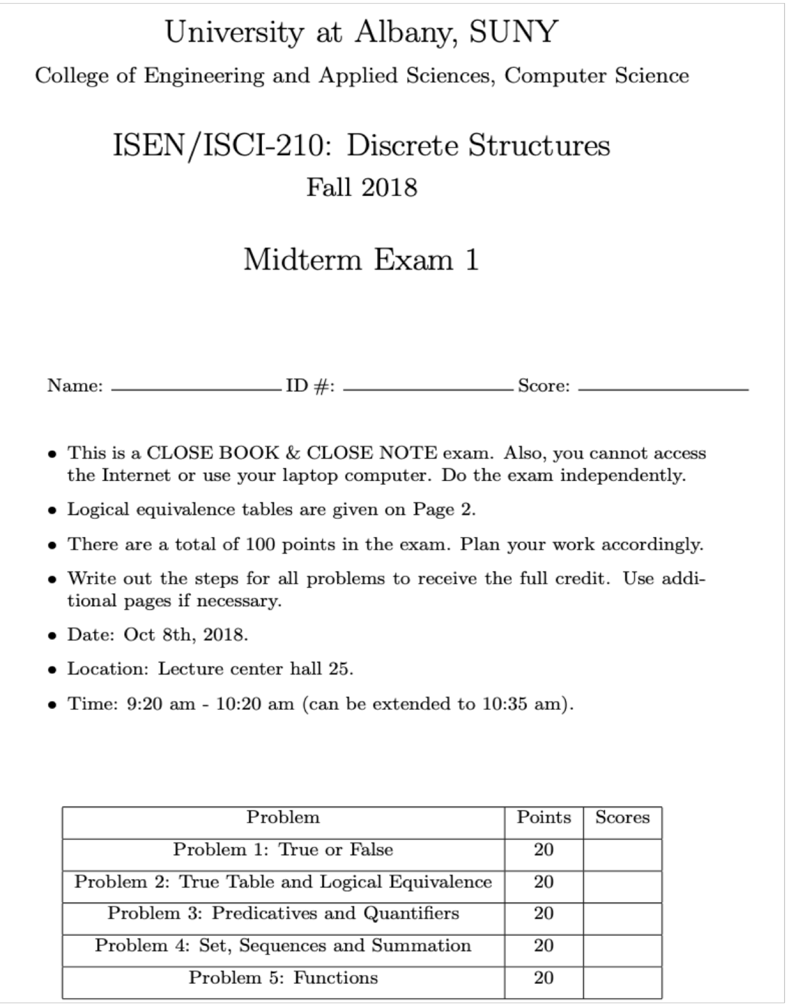
UNIVERSITY AT ALBANY

State University of New York

Lecture 19: Primes and Greatest Common Divisors

Dr. Chengjiang Long
Computer Vision Researcher at Kitware Inc.
Adjunct Professor at SUNY at Albany.
Email: **clong2@albany.edu**

About the Midterm Exam 1



University at Albany, SUNY

College of Engineering and Applied Sciences, Computer Science

ISEN/ISCI-210: Discrete Structures

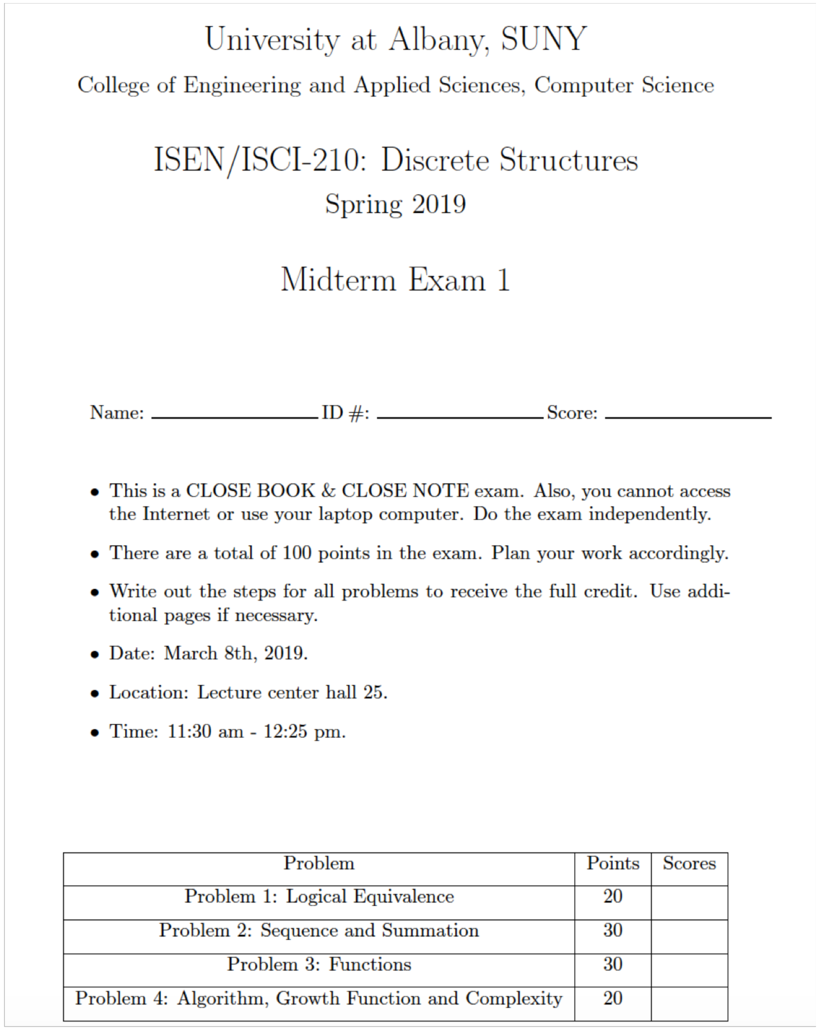
Fall 2018

Midterm Exam 1

Name: ______________ ID #: ______________ Score: ______________

- This is a CLOSE BOOK & CLOSE NOTE exam. Also, you cannot access the Internet or use your laptop computer. Do the exam independently.
- Logical equivalence tables are given on Page 2.
- There are a total of 100 points in the exam. Plan your work accordingly.
- Write out the steps for all problems to receive the full credit. Use additional pages if necessary.
- Date: Oct 8th, 2018.
- Location: Lecture center hall 25.
- Time: 9:20 am - 10:20 am (can be extended to 10:35 am).

Problem	Points	Scores
Problem 1: True or False	20	
Problem 2: True Table and Logical Equivalence	20	
Problem 3: Predicatives and Quantifiers	20	
Problem 4: Set, Sequences and Summation	20	
Problem 5: Functions	20	



University at Albany, SUNY

College of Engineering and Applied Sciences, Computer Science

ISEN/ISCI-210: Discrete Structures

Spring 2019

Midterm Exam 1

Name: ______________ ID #: ______________ Score: ______________

- This is a CLOSE BOOK & CLOSE NOTE exam. Also, you cannot access the Internet or use your laptop computer. Do the exam independently.
- There are a total of 100 points in the exam. Plan your work accordingly.
- Write out the steps for all problems to receive the full credit. Use additional pages if necessary.
- Date: March 8th, 2019.
- Location: Lecture center hall 25.
- Time: 11:30 am - 12:25 pm.

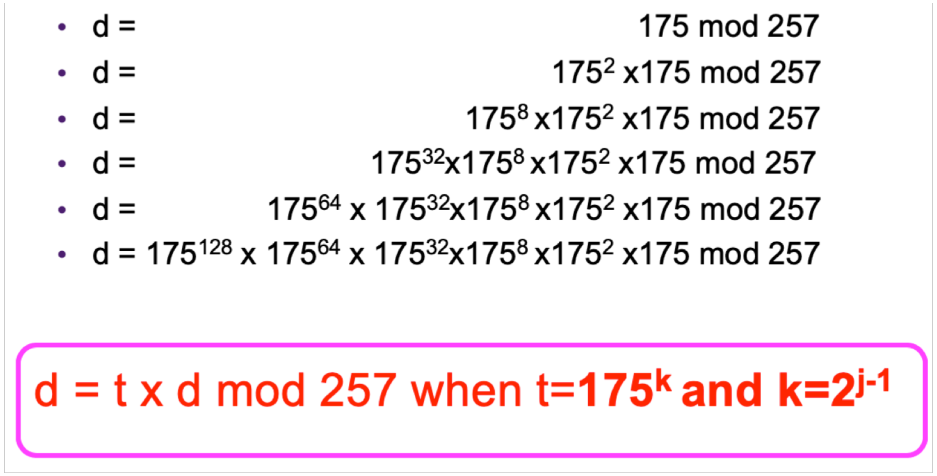
Problem	Points	Scores
Problem 1: Logical Equivalence	20	
Problem 2: Sequence and Summation	30	
Problem 3: Functions	30	
Problem 4: Algorithm, Growth Function and Complexity	20	

Attentions: No make-up tests or remote tests are offered this semester.

Recap Previous Lecture

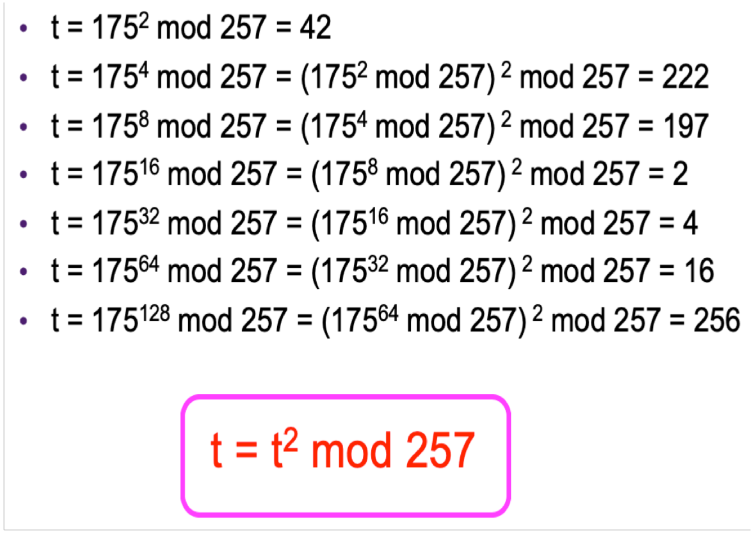
- Integer Representation, Base Conversion.
- Application: Binary Modular Exponentiation.

175^{235} mod 257



- d = 175 mod 257
- d = 175^2 x175 mod 257
- d = 175^8 x175^2 x175 mod 257
- d = 175^{32}x175^8 x175^2 x175 mod 257
- d = 175^{64} x 175^{32}x175^8 x175^2 x175 mod 257
- d = 175^{128} x 175^{64} x 175^{32}x175^8 x175^2 x175 mod 257

d = t x d mod 257 when **t=175^k and k=2^{j-1}**



- t = 175^2 mod 257 = 42
- t = 175^4 mod 257 = (175^2 mod 257)^2 mod 257 = 222
- t = 175^8 mod 257 = (175^4 mod 257)^2 mod 257 = 197
- t = 175^{16} mod 257 = (175^8 mod 257)^2 mod 257 = 2
- t = 175^{32} mod 257 = (175^{16} mod 257)^2 mod 257 = 4
- t = 175^{64} mod 257 = (175^{32} mod 257)^2 mod 257 = 16
- t = 175^{128} mod 257 = (175^{64} mod 257)^2 mod 257 = 256

t = t^2 mod 257

Outline

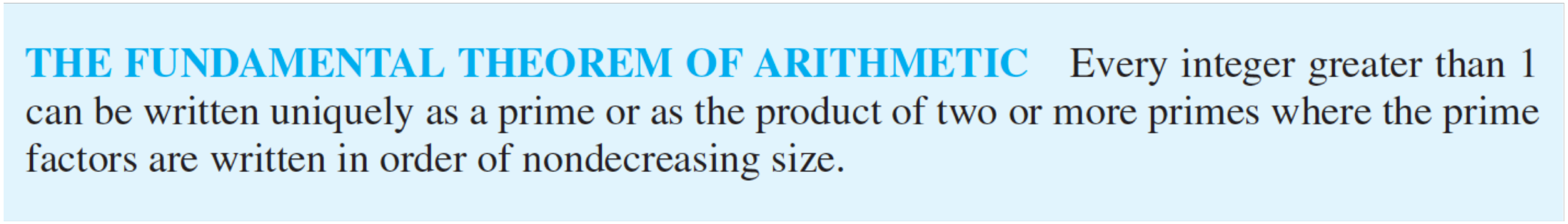
- Prime and Composite
- Prime Factorizations
- Distribution of Primes
- GCD and LCM
- Euclidean Algorithm

Outline

- **Prime and Composite**
- Prime Factorizations
- Distribution of Primes
- Greatest Common Divisor (GCD)
- Least Common Multiple (LCM)
- Euclidean Algorithm

Prime, Composite and Theorem 1

- **Prime**: a positive integer p greater than 1 if the only positive factors of p are 1 and p
- A positive integer greater than 1 that is not prime is called **composite**

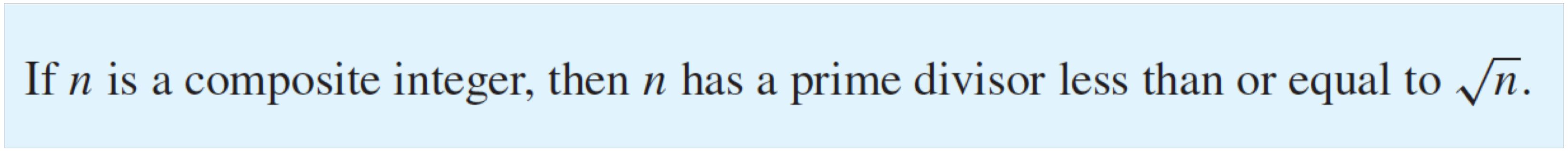


THE FUNDAMENTAL THEOREM OF ARITHMETIC Every integer greater than 1 can be written uniquely as a prime or as the product of two or more primes where the prime factors are written in order of nondecreasing size.

Example

- Prime factorizations of integers
  - $100=2\cdot2\cdot5\cdot5=2^2\cdot5^2$
  - $641=641$
  - $999=3\cdot3\cdot3\cdot37=3^3\cdot37$
  - $1024=2\cdot2\cdot2\cdot2\cdot2\cdot2\cdot2\cdot2\cdot2\cdot2=2^{10}$

Theorem 2



If n is a composite integer, then n has a prime divisor less than or equal to $\sqrt{n}$.

- As n is composite, n has a factor 1<a<n, and thus n=ab
- We show that $a \leq \sqrt{n}$ or $b \leq \sqrt{n}$ (by contraposition)
- Thus n has a divisor not exceeding $\sqrt{n}$
- This divisor is either prime or by the fundamental theorem of arithmetic, has a prime divisor less than itself, and thus a prime divisor less than less than $\sqrt{n}$
- In either case, n has a prime divisor $b \leq \sqrt{n}$

Example

- Show that 101 is prime
- The only primes not exceeding $\sqrt{101}$ are 2, 3, 5, 7.
- As 101 is not divisible by 2, 3, 5, 7, it follows that 101 is prime.

Outline

- Prime and Composite
- **Prime Factorizations**
- Distribution of Primes
- Greatest Common Divisor (GCD)
- Least Common Multiple (LCM)
- Euclidean Algorithm

Procedure for prime factorization

- Begin by diving n by successive primes, starting with 2
- If n has a prime factor, we would find a prime factor not exceeding $\sqrt{n}$.
- If no prime factor is found, then n is prime
- Otherwise, if a prime factor p is found, continue by factoring n/p

Procedure for prime factorization

- Note that n/p has no prime factors less than p
- If n/p has no prime factor greater than or equal to p and not exceeding its square root, then it is prime
- Otherwise, if it has a prime factor q, continue by factoring n/(pq)
- Continue until factorization has been reduced to a prime

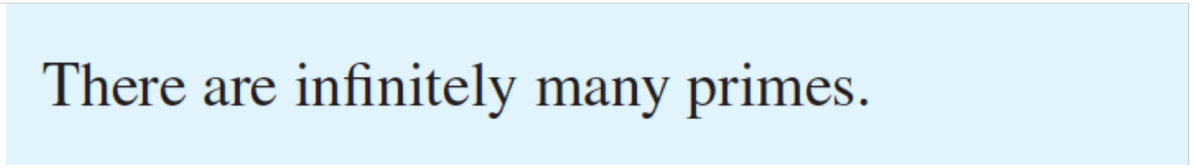
Example

- Find the prime factorization of 7007
- Start with 2, 3, 5, and then 7, 7007/7=1001
- Then, divide 1001 by successive primes, beginning with 7, and find 1001/7=143
- Continue by dividing 143 by successive primes, starting with 7, and find 143/11=13
- As 13 is prime, the procedure stops
- $7007=7 \cdot 7 \cdot 11 \cdot 13=7^2 \cdot 11 \cdot 13$

Outline

- Prime and Composite
- Prime Factorizations
- **Distribution of Primes**
- GCD and LCM
- Euclidean Algorithm

Theorem 3

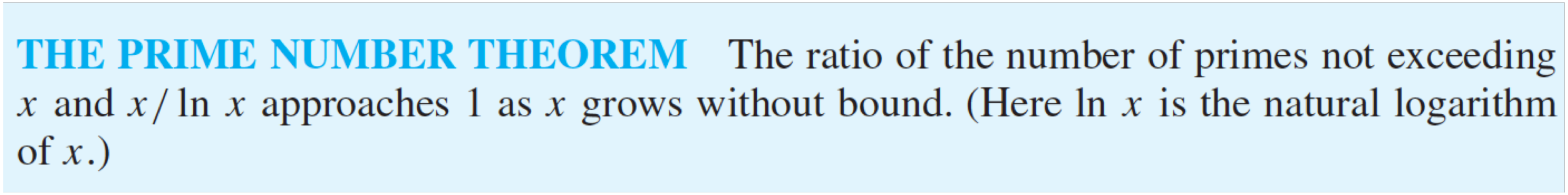

There are infinitely many primes.

- Proof by contradiction
- Assume that there are only finitely many primes, p_1, p_2, …, p_n. Let $Q=p_1p_2…p_n+1$
- By Fundamental Theorem of Arithmetic: Q is prime or else it can be written as the product of two or more primes

Mersenne primes

- Primes with the special form 2^p-1 where p is also a prime, called **Mersenne prime**.
- 2^2-1=3, 2^3-1=7, 2^5-1=31 are Mersenne primes while 2^{11}-1=2047 is not a Mersenne prime (2047=23 · 89)
- The largest Mersenne prime known (as of early 2011) is $2^{43,112,609}$-1, a number with over 13 million digits

Theorem 4



THE PRIME NUMBER THEOREM The ratio of the number of primes not exceeding x and $x/\ln x$ approaches 1 as x grows without bound. (Here $\ln x$ is the natural logarithm of x.)

- This theorem was proved in 1896 and proof is complicated.
- Can use this theorem to estimate the odds that a randomly chosen number is prime
- The odds that a randomly selected positive integer less than n is prime are approximately

  (n/ ln n)/n=1/ln n
- The odds that an integer less than 10^{1000} is prime are approximately 1/ln 10^{1000}, approximately 1/2300

Open Problems about Primes

- **Goldbach's conjecture**: every even integer n, n>2, is the sum of two primes

  4=2+2, 6=3+3, 8=5+3, 10=7+3, 12=7+5, …
- As of 2011, the conjecture has been checked for all positive even integers up to $1.6 \cdot 10^{18}$
- **Twin prime conjecture**: Twin primes are primes that differ by 2. There are infinitely many twin primes

Outline

- Prime and Composite
- Prime Factorizations
- Distribution of Primes
- **GCD and LCM**
- Euclidean Algorithm

Greatest common divisor

- Let a and b be integers, not both zero. The largest integer d such that d | a and d | b is called the **greatest common divisor** (GCD) of a and b, often denoted as gcd(a,b)
- The integers a and b are **relative prime** if their GCD is 1

  gcd(10, 17)=1, gcd(10, 21)=1, gcd(10,24)=2
- The integers a_1, a_2, …, a_n are **pairwise relatively prime** if gcd(a_i, a_j)=1 whenever $1 \le i < j \le n$

Prime factorization and GCD

- Finding GCD

$$a = p_1^{a_1} p_2^{a_2} \cdots p_n^{a_n}, b = p_1^{b_1} p_2^{b_2} \cdots p_n^{b_n}$$

$$\gcd(a,b) = p_1^{\min(a_1,b_1)} p_2^{\min(a_2,b_2)} \cdots p_n^{\min(a_n,b_n)}$$

$$120 = 2^3 \cdot 3 \cdot 5, \quad 500 = 2^2 \cdot 5^3$$

$$\gcd(120,500) = 2^2 \cdot 3^0 \cdot 5^1 = 20$$

- **Least common multiples** of the positive integers a and b is the smallest positive integer that is divisible by both a and b, denoted as lcm(a,b)

Least common multiple

- Finding LCM

$$a = p_1^{a_1} p_2^{a_2} \cdots p_n^{a_n}, b = p_1^{b_1} p_2^{b_2} \cdots p_n^{b_n}$$

$$\mathrm{lcm}(a,b) = p_1^{\max(a_1,b_1)} p_2^{\max(a_2,b_2)} \cdots p_n^{\max(a_n,b_n)}$$

$$120 = 2^3 \cdot 3 \cdot 5, 500 = 2^2 \cdot 5^3$$

$$\mathrm{lcm}(120,500) = 2^3 \cdot 3^1 \cdot 5^3 = 8 \cdot 3 \cdot 125 = 3000$$

- Let a and b be positive integers, then ab=gcd(a,b)·lcm(a,b)

Outline

- Prime and Composite
- Prime Factorizations
- Distribution of Primes
- GCD and LCM
- **Euclidean Algorithm**

Euclidean algorithm

- Need more efficient prime factorization algorithm

- Example: Find gcd(91,287)

- 287=91 · 3 +14
- Any divisor of 287 and 91 must be a divisor of 287- 91 · 3 =14
- Any divisor of 91 and 14 must also be a divisor of 287= 91 · 3
- Hence, the gcd(91,287)=gcd(91,14)

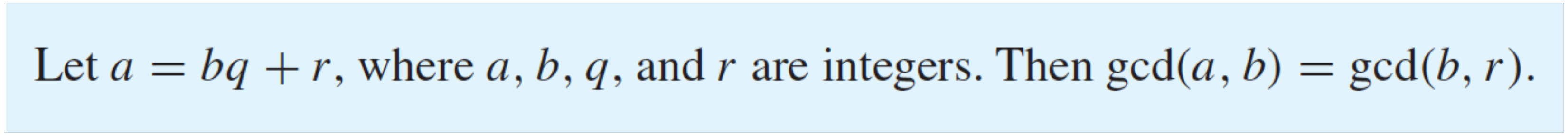
Euclidean algorithm

- Need more efficient prime factorization algorithm

- Example: Find gcd(91,287)

- gcd(91,287)=gcd(91,14)
- Next, $91= 14 \cdot 6+7$
- Any divisor of 91 and 14 also divides $91- 14 \cdot 6=7$ and any divisor of 14 and 7 divides 91, i.e., gcd(91,14)=gcd(14,7)
- $14= 7 \cdot 2$, gcd(14,7)=7,
- Thus gcd(287,91)=gcd(91,14)=gcd(14,7)=7

Euclidean algorithm



Let $a = bq + r$, where a, b, q, and r are integers. Then $\gcd(a, b) = \gcd(b, r)$.

- Proof: Suppose that d divides both a and b. Then it follows that d also divides a − bq = r. Hence, any common divisor of a and b is also a common divisor of b and r.
- Likewise, suppose that d divides both b and r. Then d also divides bq + r = a. Hence, any common divisor of b and r is also a common divisor of a and b.
- Consequently, gcd(a, b)=gcd(b,r)

Euclidean algorithm

- Suppose a and b are positive integers, a≥b. Let r_0=a and r_1=b, we successively apply the division algorithm

$$
\begin{aligned}
r_0 &= r_1 q_1 + r_2, 0 \le r_2 < r_1 \\
r_1 &= r_2 q_2 + r_3, 0 \le r_3 < r_2 \\
&\dots \\
r_{n-2} &= r_{n-1} q_{n-1} + r_n, 0 \le r_n < r_{n-1} \\
r_{n-1} &= r_n q_n \\
\gcd(a,b) &= \gcd(r_0, r_1) = \gcd(r_1, r_2) = \cdots = \gcd(r_{n-2}, r_{n-1}) \\
&= \gcd(r_{n-1}, r_n) = \gcd(r_n, 0) = r_n
\end{aligned}
$$

- Hence, the gcd is the last nonzero remainder in the sequence of divisions

Example

- Find the GCD of 414 and 662

$662=414 \cdot 1+248$

$414=248 \cdot 1+166$

$248=166 \cdot 1+82$

$166=82 \cdot 2 + 2$

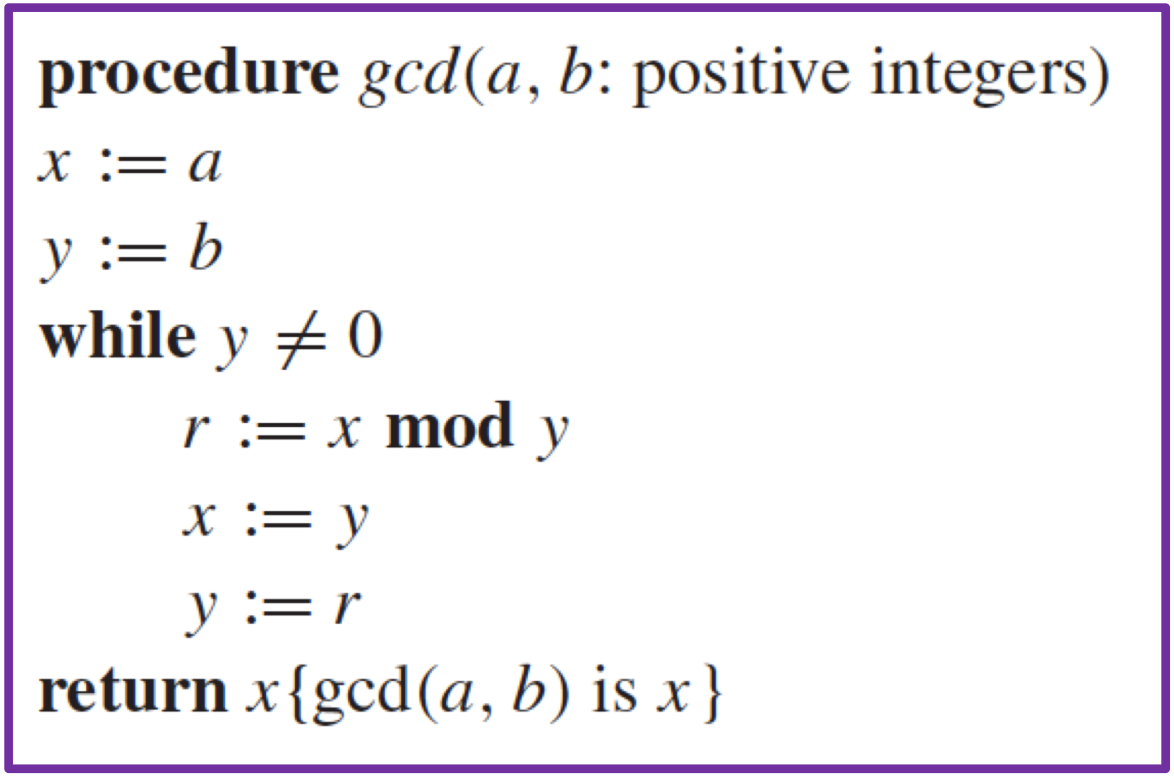
$82=2 \cdot 41$

gcd(414,662)=2 (the last nonzero remainder)

$a=bq+r$

$\gcd(a,b)=\gcd(b,r)$

The Euclidean algorithm



```
procedure $gcd(a, b$: positive integers)
$x := a$
$y := b$
while $y \neq 0$
        $r := x$ mod $y$
        $x := y$
        $y := r$
return $x$ {gcd($a, b$) is $x$}
```

- The time complexity is O(log b) (where a ≥ b)

Next class

- Topic: Cryptograph
- Pre-class reading: Chap 5.6