Lectures 21-22: Primes and Greatest Common Divisor

Jingjin Yu |Computer Science @ Rutgers

RUTGERS
THE STATE UNIVERSITY OF NEW JERSEY

November 20, 2020

Algorithmic Robotics & Control Lab

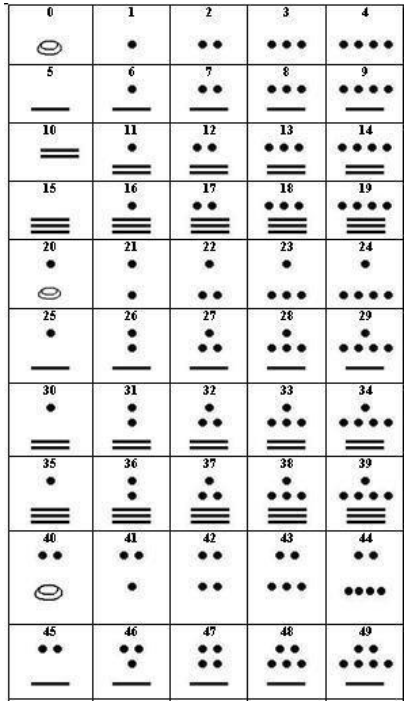
Outline

- Lecture 20 review
- Prime numbers
  - Primality and checking primality
    - Fundamental theorem of arithmetic (FTA)
    - Algorithm for prime factorization
  - Properties of primes
- Greatest common divisor and least common multiple
  - Euclid's algorithm
  - Euclid's lemma
  - Proving the uniqueness statement in FTA

- A repeating note: **make sure you read the textbook**

L20: Representing Integers

- For everyday: decimals are **base 10** representations.
  - **Ex**: $12345, \quad 22222, \quad 42$
  - **Ex**: $3.1415926 \ldots$
  - Why do we use decimal numbers?
  - Mayans use base 20 and base 5
- We can use any positive integer as the base
  - Base 1: unary numbers, e.g., $(1111111)_1$
  - Base 2: binary numbers, e.g., $(0010\ 1110)_2$
  - Base 3: ternary
  - Base 8: octal
  - Base 16: hexadecimal



L20: Algorithm for Base Conversion

- **Theorem.** Let $b > 1$ and n be positive integers. Then n may be represented as

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

in a **unique** way, in which $0 \leq a_0, \ldots, a_k < b$ and $a_k \neq 0$.

- **Algorithm** for converting from base b to base 10: simply compute the polynomial!
- **Ex:** $(101011111)_2$ to base 10
- **Ex:** $(7016)_8$ to base 10
- **Ex:** $(A7E)_{16}$ to base 10

L20: Convert from Base 10 to Base b

- **Algorithm** for converting from base 10 to base b: Given n, $n = n_0 b + r_0$ for some $0 \leq r_0 < b$, r_0 is the last digit. Then, repeat the same with n_0 to obtain $n_0 = n_1 b + r_1$, until we reach $n_k = 0$. The base b number is $(r_k \ldots r_0)_b$

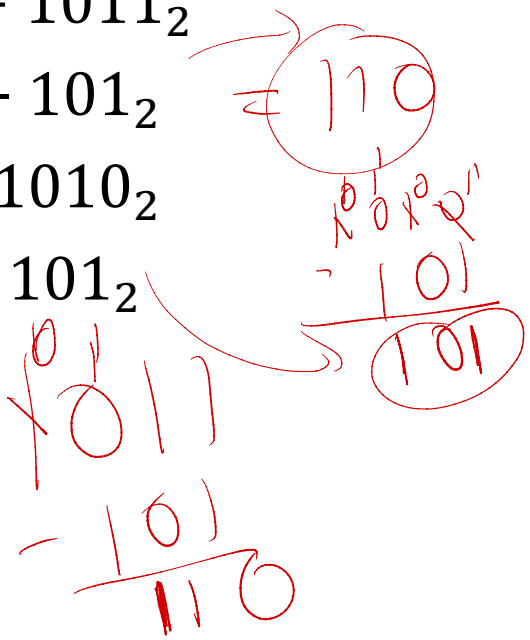
- **Ex**: Convert 12345 to octal.
- **Ex**: Convert 37 to binary.

L20: Between Binary, Octal, Hexadecimal

- **Ex**: Convert $(110\ 0011)_2$ to octal.
- **Ex**: Convert $(56)_8$ to binary.
- **Ex**: Convert $(1110\ 1011)_2$ to hexadecimal and back.

L20: Binary Arithmetic Algorithms

- **Ex:** $1110_2 + 1011_2$
- **Ex:** $1011_2 - 101_2$
- **Ex:** $101_2 - 1010_2$
- **Ex:** $1110_2 * 101_2$



L20: Modular Exponentiation

- **Ex:** $5^{11} \bmod 7$

Primes and Checking Primality

- **Def^n**: An integer $p > 1$ is a **prime** if its only positive factors are 1 and p. Otherwise, p is a composite
- **Ex**: 7 is a prime. 15 is not.
- **Lemma 1**. If $n > 1$ is a composite, then n has a prime factor of no more than $\sqrt{n}$.

Proof. Suppose n only has factors $> \sqrt{n}$ say

$n = f_1 \cdot f_1 \cdots$ w/ $f_i > \sqrt{n}$

$n = f_1 \cdot f_2 \cdots \geq \sqrt{n} \cdot \sqrt{n} \cdots = n$

Contradiction

Checking Primality: Example

- **Ex:** Is 101 prime?

$\lfloor \sqrt{101} \rfloor = 10$, need to check all prime #s $\in [2, 10]$
these 2, 3, 5, 7

$101 = 50 \times 2 + 1$

$101 = 33 \times 3 + 2$

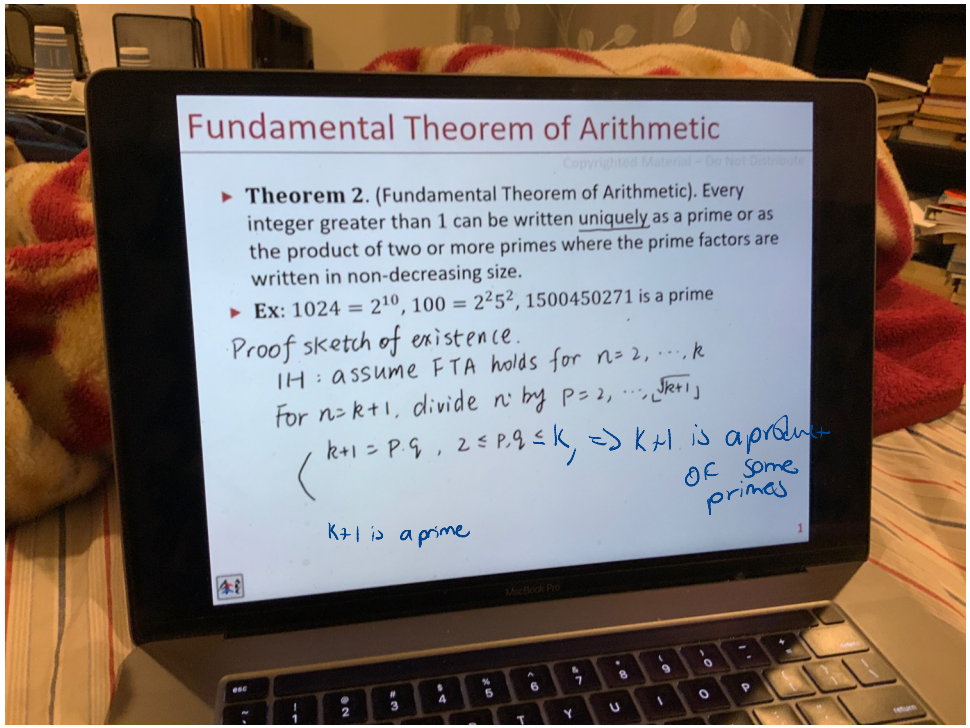
$101 = 20 \times 5 + 1$

$101 = 7 \times 14 + 3$

101 is a prime

Fundamental Theorem of Arithmetic

- **Theorem 2**. (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 non-decreasing size.
- **Ex**: $1024 = 2^{10}$, $100 = 2^2 5^2$, 1500450271 is a prime



Prime Factorization

- **Algorithm**. (Prime Factorization). To factorize n or determine it is a prime, let $n_1 = n$. Starting with $i = 1$, do
  1) Let the prime numbers $\leq \sqrt{n_1}$ be $p_1 = 2, p_2 = 3, \ldots$
  2) Test whether $p_j \mid n_i$ starting from $j = 1,2, \ldots$ two possibilities
  3) If for some j, $p_j \mid n_i$, let $n_{i+1} = \frac{n_i}{p_j}$ and $q_i = p_j$. Go to 1) with $i = i + 1$
  4) Let $q_i = n_i$. All the q_i collected so far are the prime factors

- **Ex**: Factor $n = 126$

1) $n_1 = 126$ $p_1 = 2, p_2 = 3, p_3 = 5, p_4 = 7, p_5 = 11$

2) $p_1 \mid n_1$

3) $n_2 = \frac{n_1}{2} = 63$, $q_1 = 2$

1) $n_2 = 63$

2) $p_2 \mid n_2$

3) $n_3 = \frac{n_2}{3} = 21$, $q_2 = 3$

1) $n_3 = 21$

2) $p_2 \mid n_3$

3) $n_4 = \frac{n_3}{3} = 7$, $q_3 = 3$

1) $n_4 = 7$, $p_1 = 2$

2) $p_1 \nmid 7$

4) $q_4 = 7$

$q_1 = 2, q_2 = 3, q_3 = 3$

$q_4 = 7$

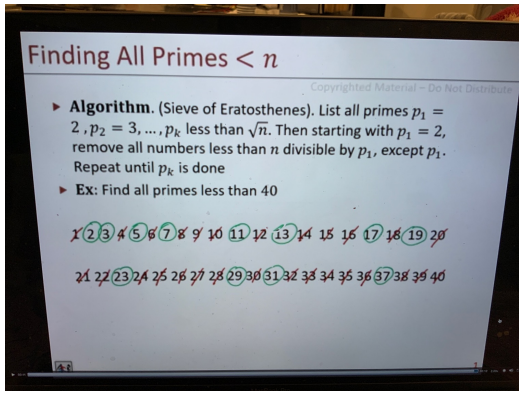
$126 = 2 \cdot 3^2 \cdot 7$

Finding All Primes $< n$

- **Algorithm**. (Sieve of Eratosthenes). List all primes $p_1 = 2, p_2 = 3, \ldots, p_k$ less than $\sqrt{n}$. Then starting with $p_1 = 2$, remove all numbers less than n divisible by p_1, except p_1. Repeat until p_k is done
- **Ex**: Find all primes less than 40

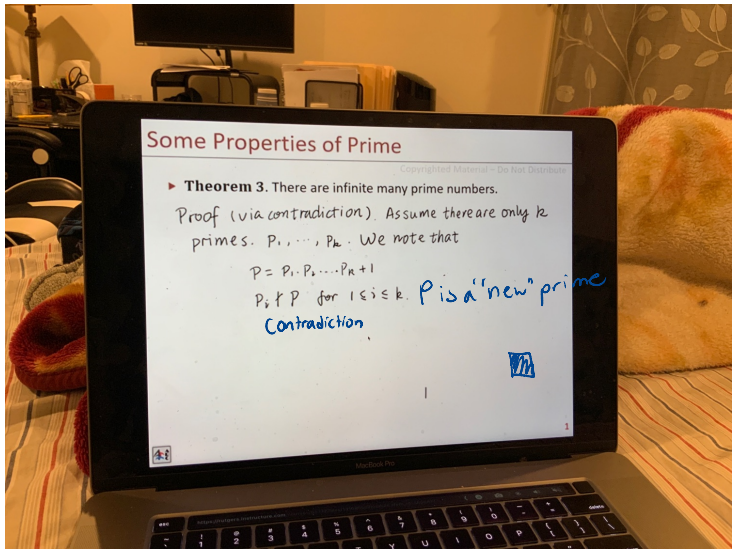
1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20

21 22 23 24 25 26 27 28 29 30 31 32 33 34 35 36 37 38 39 40



Some Properties of Prime

- **Theorem 3**. There are infinite many prime numbers.



1.6×10^{18} | Chen(1973) $n = P_1 + t^{12/5}$ | Ramare(1995)

- **Conjecture 4**. Every even number greater than two is the sum of two prime numbers Goldbach's Conjecture
- **Conjecture 5**. There are infinitely many prime pairs (p_1, p_2) such that $p_1 - p_2 = 2$. 70m Zhang(2013) | 246

GCD and LCM

- **Def^n**: Let $a \neq b$ be integers. The largest d such that $d \mid a$ and $d \mid b$ is the **greatest common divisor** of a and b, or $\gcd(a, b)$.
- **Ex**: $\gcd(35, 28) = 7$
- **Ex**: $\gcd(5, 22) = 1$

- **Def^n**: Integers a and b are **relatively prime** if $\gcd(a, b) = 1$.
- **Ex**: 5 and 22 are relative primes.

- **Def^n**: The **least common multiple** of positive integers a and b is the smallest positive integer that is divisible by a and b, denoted as $\text{lcm}(a, b)$.
- **Ex**: $\text{lcm}(3, 6) = 6$
- **Ex**: $\text{lcm}(4, 5) = 20$

GCD and LCM, Cont.

- **Theorem 6.** For positive integers a and b,

$$ab = \gcd(a, b) \cdot \text{lcm}(a, b)$$

- **Ex:** $a = 180, b = 70$

$180 = 2 \times 90 = 2 \times 2 \times 45 = 2^2 \times 3 \times 15 = 2^2 \times 3 \times 3 \times 5 = 2^2 3^2 5$

$\gcd(180, 70) = 10$

$\text{lcm}(180, 70) = 10 \cdot 2 \cdot 3^2 \cdot 7 = 1260$

$180 \cdot 70 = \gcd(180, 70) \cdot \text{lcm}(180, 70)$

Euclid's Algorithm

- **Lemma 7.** Let $a = bq + r$ where a, b, q, and r are integers. Then $\gcd(a, b) = \gcd(b, r)$
  - Proof: $d = \gcd(a, b) \Rightarrow d|a, d|b \Rightarrow d|-bq \Rightarrow d|(a - bq) \Rightarrow d|r$
- **Algorithm.** Let $r_0 = a > r_1 = b$
  - $r_0 = r_1 q_1 + r_2, 0 < r_2 < r_1$
  - $r_1 = r_2 q_2 + r_3, 0 < r_3 < r_2$
  - …
  - $r_{n-2} = r_{n-1}\, q_{n-1} + r_n, 0 < r_3 < r_2$
  - $r_{n-1} = r_n q_n$
  - $\gcd(a, b) = \gcd(r_0, r_1) = \gcd(r_1, r_2) = \cdots = \gcd(r_{n-1}, r_n) = r_n$

Euclid's Algorithm: Example

- **Ex**: Compute $\gcd(662, 414)$

$662 = 414 \cdot 1 + 248$

$414 = 248 \cdot 1 + 166$

$248 = 166 \cdot 1 + 82$

$166 = 82 \cdot 2 + 2$

$82 = 2 \cdot 41$

$\gcd(662, 414) \Rightarrow 2$

$123 = 46(2) + 31$

$46 = 1 \cdot 46$

123, 46

$1 = 123 + 46t$

615

$1 = 123(3) +$

$\frac{1 - 123(3)}{46} = t$

$\frac{1-123}{t}$

$123 = 76x + d$

Euclid's Lemma, I

- **Theorem 8**: If a and b are positive integers, then there exists integers s, t such that $\gcd(a, b) = sa + tb$

gcd (662, 414)

662 = 414 · 1 + 248

414 = 248 · 1 + 166

248 = 166 · 1 + 82

166 = 82 · 2 + 2

82 = 41 · 2

2 = 166 − 82 · 2

= 166 − (248 − 166) · 2

= 166 · 3 − 248 · 2

= (414 − 248) · 3 − 248 · 2

= 414 · 3 − 248 · 5 = 414 · 3 − (662 − 414) · 5

= 414 · 8 − 662 · 5

s = −5, t = 8

- **Corollary 9**: If $\gcd(a, b) = 1$, then $\exists s, t, sa + tb = 1$.

Euclid's Lemma, II

- **Corollary 9**: If $\gcd(a, b) = 1$, then $\exists s, t, sa + tb = 1$.
- **Lemma 10**. (Euclid's lemma). Let p be a prime. For integers a and b, if $p \mid ab$, then $p \mid a$ or $p \mid b$

Proof. WLOG, assume $p \nmid a$, we want to show $p \mid b$

$p \nmid a$, p is prime $\Rightarrow \gcd(p, a) = 1$

$\Rightarrow \exists s, t,\ sp + ta = 1$

$\overset{*b}{\Rightarrow}$ $spb + tab = b$ | $p \mid spb$, $p \mid ab$, $p \mid tab$

$p \mid (spb + tab) \Rightarrow p \mid b$

Uniqueness of Fund. Thm. Of Arithmetic

- **Theorem 2**. (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 non-decreasing size.