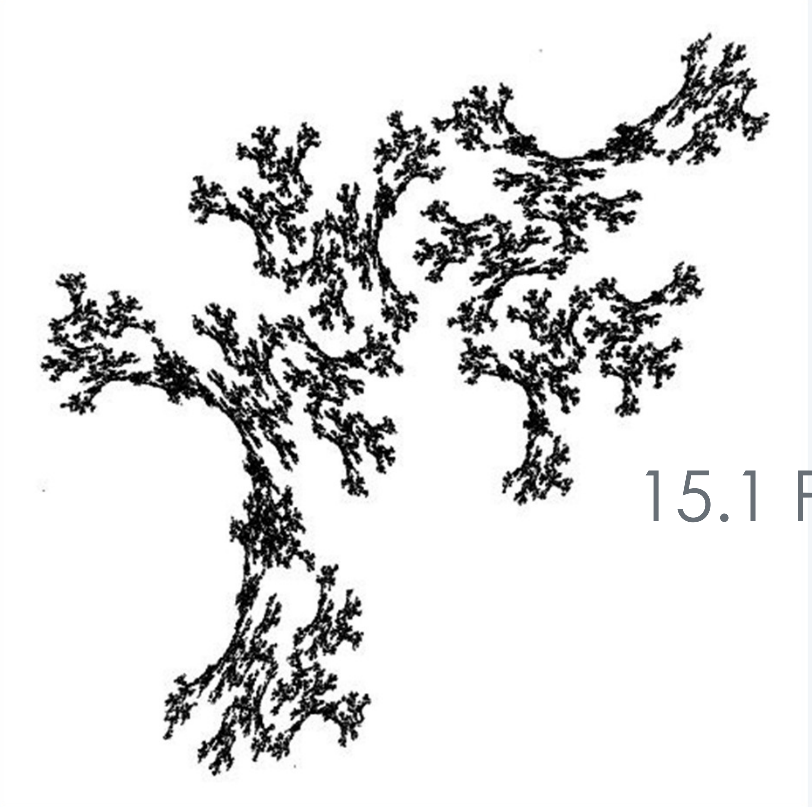
INTRODUCTION TO
DISCRETE STRUCTURES

15.1 Primes and GCD

1.1–1.2



15.1 Primes and GCD

- Introduction
- Fundamental theorem of Arithmetic
- Distribution of Primes
- GCD and LCM
- Euclidean Algorithm

Definition

An integer n is prime, if and only if 1 and n are its only divisors

An integer that is not prime is called a composite number.

Finding all primes less than n

1. List all numbers less than n

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

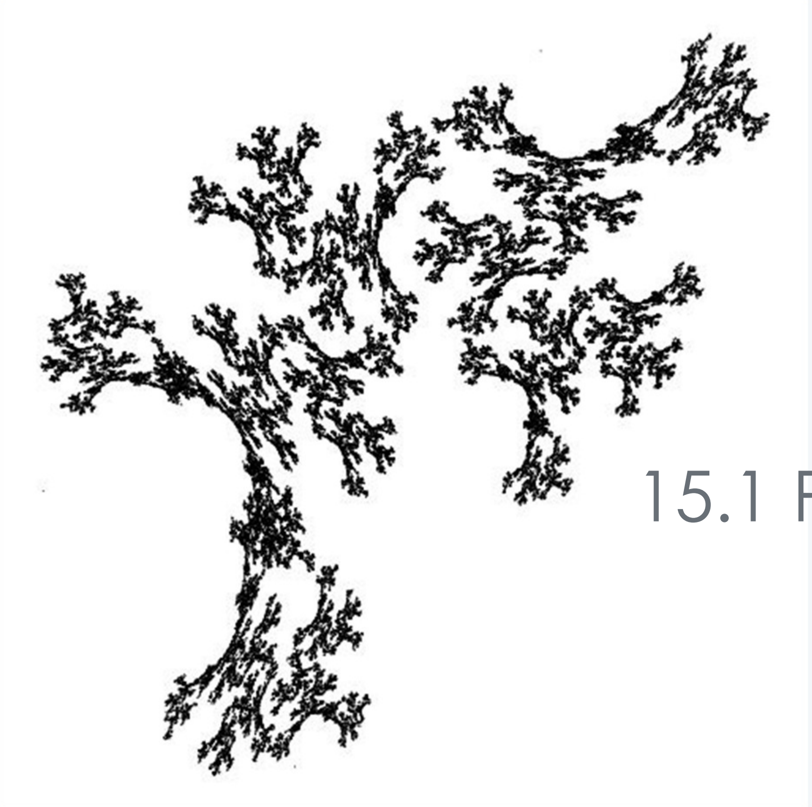
31 32 33 34 35 36 37 38 39 40

41 42 43 44 45 46 47 48 49 50

Remove all even integers except 2

Remove all multiples of 3 except 3

Continue…



INTRODUCTION TO DISCRETE STRUCTURES

15.1 Primes and GCD

- Introduction
- Fundamental theorem of Arithmetic
- Distribution of Primes
- GCD and LCM
- Euclidean Algorithm

Theorem

Every integer greater than 1 can be written uniquely as a prime or a product of primes written in the order of non-decreasing size.

Prime factorization is unique

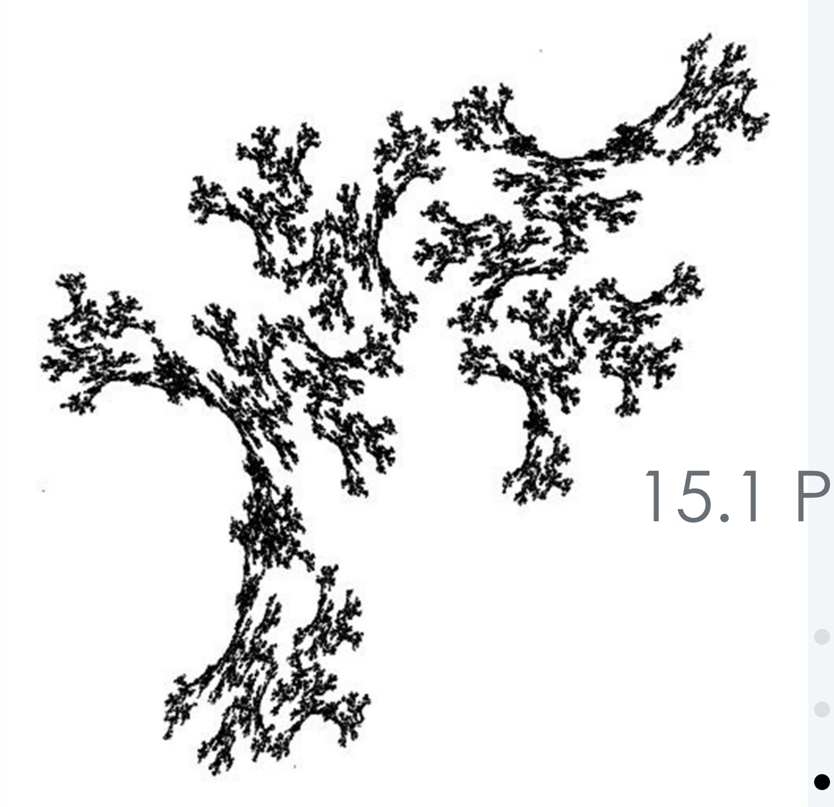
Proof.

Theorem

If n is a composite integer, then n has a prime divisor less or equal to sqrt(n)

Proof.

Fact. To find all prime factors of n, we only need to divide n by integers up to sqrt(n)



INTRODUCTION TO
DISCRETE STRUCTURES

15.1 Primes and GCD

- Introduction
- Fundamental theorem of Arithmetic
- Distribution of Primes
- GCD and LCM
- Euclidean Algorithm

Theorem

There are infinitely many prime numbers

How many primes are there?

Science News

The Great Internet Mersenne Prime Search (GIMPS) has discovered the largest known prime number, $2^{77,232,917}-1$, having 23,249,425 digits. A computer volunteered by Jonathan Pace made the find on December 26, 2017. Jonathan is one of thousands of volunteers using free GIMPS software.

Prime Number Theorem

The number of primes not exceeding x is approximately x / ln(x)

Question. What is the chance that a randomly selected number n is prime?

Conjectures

Conjecture. Every even integer > 4 can be written as a sum of two prime numbers

This is only a conjecture, and no one has proved this yet

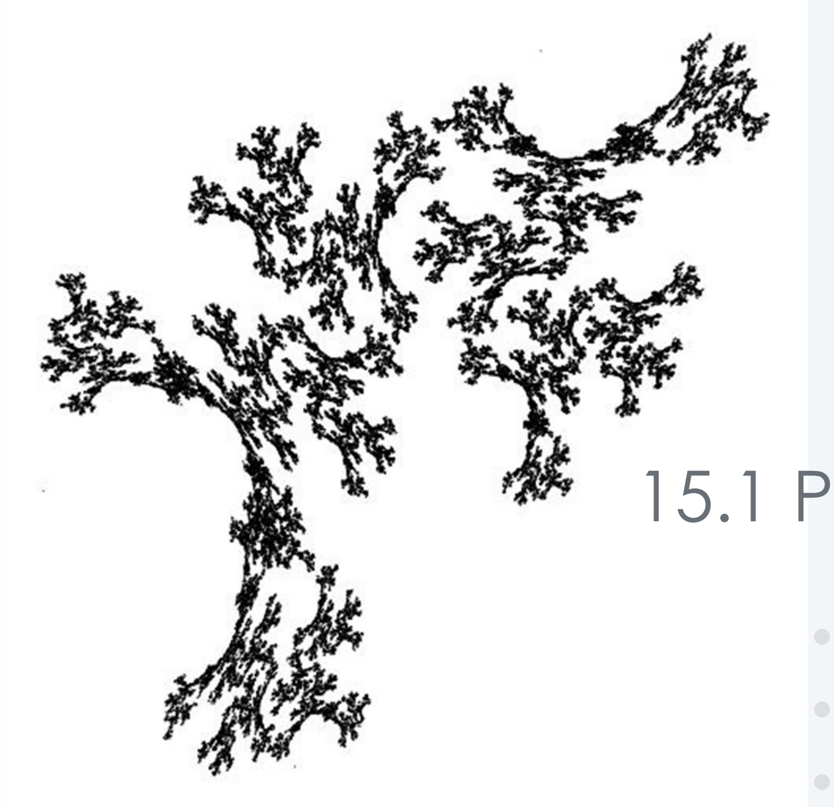
Another Conjecture. Every odd integer > 5 is the sum of three prime numbers

Twin Prime Conjecture. There are infinitely many twin primes (3 and 5, 7 and 9 etc)

Cousin Prime Conjecture. p and p + 4 are primes

Largest Twin primes found so far. $2996863034895 \cdot 2^{1290000} \pm 1$,[19] with 388,342 decimal digits*

* Source: Wikipedia



INTRODUCTION TO DISCRETE STRUCTURES

15.1 Primes and GCD

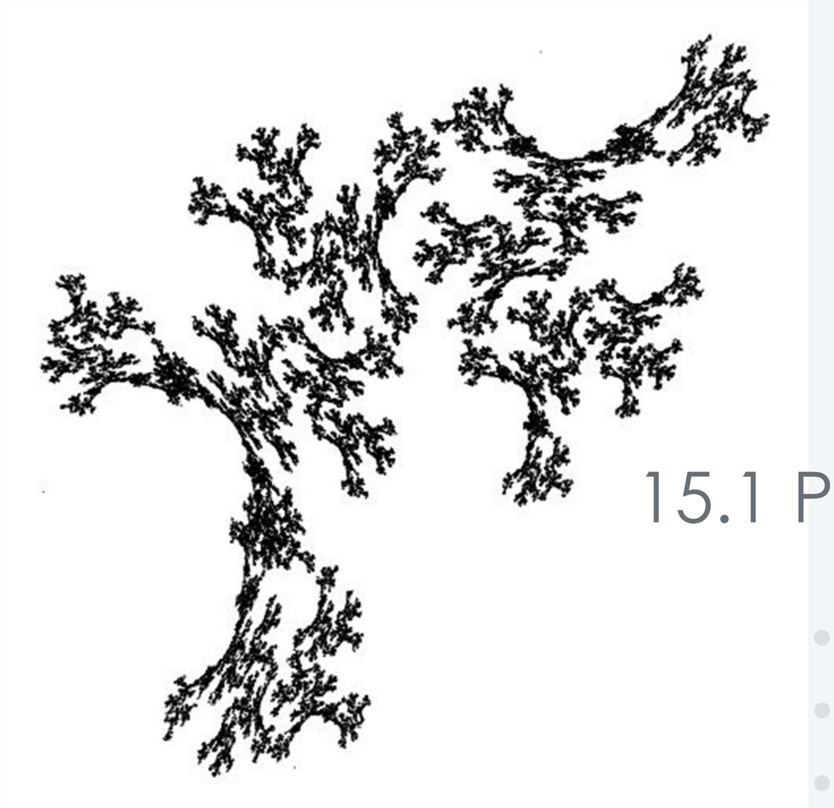
- Introduction
- Fundamental theorem of Arithmetic
- Distribution of Primes
- GCD and LCM
- Euclidean Algorithm

GCD and LCM

Greatest Common Divisor (GCD) – is the largest number that divides both a and b

Least Common Multiple (LCM) – Is the smallest positive integer that is divisible by a and b

INTRODUCTION TO DISCRETE STRUCTURES



15.1 Primes and GCD

- Introduction
- Fundamental theorem of Arithmetic
- Distribution of Primes
- GCD and LCM
- Euclidean Algorithm

DO NOT DISTRIBUTE

GCD as a linear combination

If a and b are positive integers, the gcd(a, b) can be written as gcd(a, b) = am + bn for some integers m and n.

Note. Multiples of GCD are Linear Combinations of a and b

E.g. write gcd(312, 125) as a linear combination 312 m + 125 n

Euclidean Algorithm

$$\begin{aligned} gcd(a,) &= gcd(a\%b, b) && \text{if } a > b \\ &= gcd(a, b\%a) && \text{if } b > a \\ &= a \ \ (\text{or } b) && \text{if } a = b \end{aligned}$$

Lemmas

Lemma 1. If a, b, c > 0 such that a and b are relatively prime, then if a | (bc) ➔ a | c

Theorem

If p is prime and $p \mid a_1 a_2 \ldots a_n$, then $p \mid a_i$ for some i

Lemma. Prove if $p \mid (ab)$ then $p \mid a$ or $p \mid b$

Theorem

If p is prime and $p \mid a_1 a_2 \ldots a_n$, then $p \mid a_i$ for some i