Introduction: Greatest Common Divisors I

Daniel Kane

Department of Computer Science and Engineering
University of California, San Diego

Algorithmic Design and Techniques
Algorithms and Data Structures at edX

Learning Objectives

- Define greatest common divisors.
- Compute greatest common divisors inefficiently.

GCDs

- Put fraction $\frac{a}{b}$ in simplest form.
- Divide numerator and denominator by d, to get $\frac{a/d}{b/d}$.

GCDs

- Put fraction $\frac{a}{b}$ in simplest form.
- Divide numerator and denominator by d, to get $\frac{a/d}{b/d}$.
    - Need d to divide a and b.
    - Want d to be as large as possible.

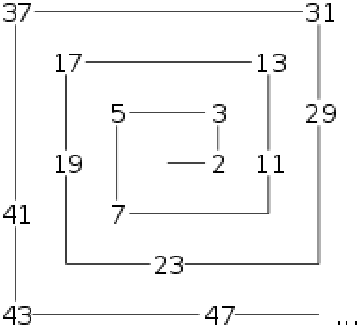
GCDs

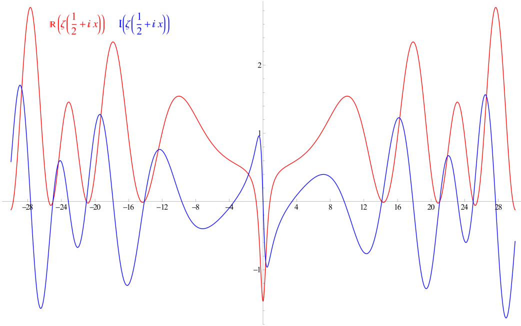
- Put fraction $\frac{a}{b}$ in simplest form.
- Divide numerator and denominator by d, to get $\frac{a/d}{b/d}$.
  - Need d to divide a and b.
  - Want d to be as large as possible.

Definition

For integers, a and b, their greatest common divisor or $\gcd(a, b)$ is the largest integer d so that d divides both a and b.

Number Theory





Cryptography

Computation

Compute GCD

Input: Integers $a, b \geq 0$.

Output: $\gcd(a, b)$.

Computation

Compute GCD

Input: Integers $a, b \geq 0$.

Output: $\gcd(a, b)$.

Run on large numbers like

$$\gcd(3918848, 1653264).$$

Naive Algorithm

```
Function NaiveGCD(a, b)

best ← 0
for d from 1 to a + b:
    if d|a and d|b:
        best ← d
return best
```

Naive Algorithm

Function NaiveGCD(a, b)

$best \leftarrow 0$
for d from 1 to $a + b$:
  if $d|a$ and $d|b$:
    $best \leftarrow d$
return $best$

- Runtime approximately $a + b$.
- Very slow for 20 digit numbers.