COMP8760 Lecture - 2

Modular Arithmetic, Prime Factorisation, Euclidean Algorithm, Mutually Prime

Sanjay Bhattacherjee

University of Kent

bsdqm9

Outline

Modular Arithmetic

- $+ \pmod{N}$ and $\times \pmod{N}$

Prime Factorisation

- Decompose an integer into prime numbers
- LCM is found by considering the maximum of the two exponents for a prime
- GCD is found by considering the minimum of the two exponents for a prime

Euclidean Algorithm

- A very efficient way to find GCD, without computing the prime factorisations

Mutually Prime Numbers

- When they have no common factors > 1
- In other words, when their GCD is 1

Resources

Study Material

Book 1 *Cryptography Made Simple*
Author Nigel P. Smart.
Link to eBook

Section 1.1 Modular Arithmetic
Section 1.3.1 Greatest Common Divisors
Section 1.3.2 The Euclidean Algorithm
Section 2.1 Prime Numbers
Section 2.2 Factoring
Section 2.3.1 Trial Division
Section 1.1.3 Euler's ϕ Function

Reminder: Solve the Practice Worksheet!

Solution of the practice worksheet corresponding to Lecture 1 is on Moodle.

Outline

Modular Arithmetic (Cointinued)

Prime numbers, GCD and LCM
- Prime numbers
- LCM and GCD

Euclidean Algorithm

Mutually Prime
- Euler's phi function: $\phi(n)$

$$\mathbb{Z}_N =: \text{set of remainders of } N$$

$$\mathbb{Z}_N = \{0, 1, 2, 3, \ldots, N-1\}$$

Set of Remainders

$$\mathbb{Z}_N =: \text{set of remainders of } N$$

$$\mathbb{Z}_N = \{0, 1, 2, 3, \ldots, N-1\}$$

Some examples:

$\mathbb{Z}_2 = \{0, 1\}$
$\mathbb{Z}_7 = \{0, 1, 2, 3, 4, 5, 6\}$
$\mathbb{Z}_{11} = \{0, 1, 2, 3, 4, 5, 6, 7, 8, 9, 10\}$
$\mathbb{Z}_{1001} = \{0, 1, \ldots, 1000\}$

The $\pmod{}$ operator

We define

$$a \pmod{N} = \underline{r}$$

remainder

This operator gives the remainder on dividing the integer a with N.

The $\pmod{}$ operator

We define

$$a \pmod{N} = \underline{\mathrm{r}}$$

remainder

This operator gives the remainder on dividing the integer a with N.

Examples

- $13 \pmod{5} = 3$

bsdqm9

The $\pmod{}$ operator

We define

$$a \pmod{N} = \underline{r}$$

remainder

This operator gives the remainder on dividing the integer a with N.

Examples

- $13 \pmod{5} = 3$
- $112 \pmod{7} = 0$

Congruent $\pmod N$

When $x - y$ is a multiple of N, we define

$$x = y \pmod N.$$

In other words, integers x and y both have the same remainder on dividing with N.

Congruent $\pmod N$

When $x - y$ is a multiple of N, we define

$$x = y \pmod N.$$

In other words, integers x and y both have the same remainder on dividing with N.

Examples

- $8 = 13 \pmod 5$

Congruent $\pmod{N}$

When $x - y$ is a multiple of N, we define

$$x = y \pmod{N}.$$

In other words, integers x and y both have the same remainder on dividing with N.

Examples

- $8 = 13 \pmod{5}$
- $21 = 112 \pmod{7}$

Modular Addition

We define

$$(x \quad + \quad y) \qquad \pmod{N} \ =$$

Modular Addition

We define

$$(x + y) \pmod{N} =$$

$$z \pmod{N} =$$

bsdqm9

University of Kent

Modular Addition

We define

$$(x + y) \pmod{N} =$$

$$z \pmod{N} = \underline{r} \in \mathbb{Z}_N$$

remainder

Modular Addition

We define

$$(x + y) \pmod N =$$

$$z \pmod N = \underline{r} \in \mathbb{Z}_N$$

remainder

This operator gives the remainder on dividing $z = (x + y)$ with N.

Modular Addition

We define

$$(x \quad + \quad y) \quad \pmod{N} =$$

$$z \quad \pmod{N} = \underline{r} \quad \in \mathbb{Z}_N$$

remainder

This operator gives the remainder on dividing $z = (x + y)$ with N.

$(6 + 7) \pmod{5}$

Modular Addition

We define

$$(x + y) \pmod N =$$

$$z \pmod N = \underline{r} \in \mathbb{Z}_N$$

remainder

This operator gives the remainder on dividing $z = (x + y)$ with N.

$$(6+7) \pmod 5 \qquad = 13 \pmod 5$$

University of Kent

Modular Addition

We define

$$(x + y) \pmod{N} =$$

$$z \pmod{N} = \underline{r} \in \mathbb{Z}_N$$

remainder

This operator gives the remainder on dividing $z = (x + y)$ with N.

$$(6 + 7) \pmod{5} \quad = 13 \pmod{5} \quad = 3 \in \mathbb{Z}_5$$

Modular Addition

We define

$$(x + y) \pmod{N} =$$

$$z \pmod{N} = \underline{r} \in \mathbb{Z}_N$$

remainder

This operator gives the remainder on dividing $z = (x + y)$ with N.

$(6 + 7) \pmod 5 \quad = 13 \pmod 5 \quad = 3 \in \mathbb{Z}_5$

$(62 + 50) \pmod 7$

bsdqm9

University of Kent

Modular Addition

We define

$$(x \quad + \quad y) \quad \pmod{N} =$$

$$z \quad \pmod{N} = \underbrace{r}_{\text{remainder}} \quad \in \mathbb{Z}_N$$

This operator gives the remainder on dividing $z = (x + y)$ with N.

$$(6 + 7) \pmod{5} \quad = 13 \pmod{5} \quad = 3 \in \mathbb{Z}_5$$

$$(62 + 50) \pmod{7} \quad = 112 \pmod{7}$$

bsdqm9

Modular Addition

We define

$$(x + y) \pmod{N} =$$

$$z \pmod{N} = \underline{r} \in \mathbb{Z}_N$$

remainder

This operator gives the remainder on dividing $z = (x + y)$ with N.

$$(6 + 7) \pmod{5} = 13 \pmod{5} = 3 \in \mathbb{Z}_5$$

$$(62 + 50) \pmod{7} = 112 \pmod{7} = 0 \in \mathbb{Z}_7$$

Modular Addition in $\mathbb{Z}_5$

For any two integers x and y,

$$x + y \pmod{N} \in \{0, 1, 2, 3, 4\}.$$

Modular Addition in $\mathbb{Z}_5$

For any two integers x and y,

$$x + y \pmod{N} \in \{0, 1, 2, 3, 4\}.$$

The following table shows the results of additions $\pmod{N}$ of all elements of $\mathbb{Z}_5$ with each other.

Modular Addition in $\mathbb{Z}_5$

For any two integers x and y,

$$x + y \pmod N \in \{0, 1, 2, 3, 4\}.$$

The following table shows the results of additions $\pmod N$ of all elements of $\mathbb{Z}_5$ with each other.

Addition $\pmod 5$ in $\mathbb{Z}_5$

	0	1	2	3	4
0	0	1	2	3	4
1	1	2	3	4	0
2	2	3	4	0	1
3	3	4	0	1	2
4	4	0	1	2	3

Modular Multiplication

We define

$$(x \times y) \pmod{N} =$$

bsdqm9

Modular Multiplication

We define

$$(x \quad \times \quad y) \qquad \pmod{N} \;=$$

$$z \pmod{N} \;=$$

bsdqm9

Modular Multiplication

We define

$$(x \quad \times \quad y) \quad \pmod{N} \; =$$

$$z \pmod{N} \; = \; \underline{r} \qquad \in \mathbb{Z}_N$$

remainder

bsdqm9

University of Kent

Modular Multiplication

We define

$$(x \times y) \pmod N = z \pmod N = \underline{r} \in \mathbb{Z}_N$$

remainder

This operator gives the remainder on dividing $z = (x \times y)$ with N.

Modular Multiplication

We define

$$(x \quad \times \quad y) \quad \pmod N \;=$$

$$z \pmod N \;=\; \underline{r} \qquad \in \mathbb{Z}_N$$

remainder

This operator gives the remainder on dividing $z = (x \times y)$ with N.

$(6 \times 7) \pmod 5)$

Modular Multiplication

We define

$$(x \times y) \pmod{N} =$$

$$z \pmod{N} = \underline{r} \in \mathbb{Z}_N$$

remainder

This operator gives the remainder on dividing $z = (x \times y)$ with N.

$$(6 \times 7) \pmod 5 \qquad = 42 \pmod 5$$

Modular Multiplication

We define

$$(x \quad \times \quad y) \pmod N =$$

$$z \pmod N = \underline{r} \quad \in \mathbb{Z}_N$$

remainder

This operator gives the remainder on dividing $z = (x \times y)$ with N.

$$(6 \times 7) \pmod 5 \qquad = 42 \pmod 5 \quad = 2 \in \mathbb{Z}_5$$

Modular Multiplication

We define

$$(x \times y) \pmod N =$$

$$z \pmod N = \underbrace{\underline{r}}_{\text{remainder}} \in \mathbb{Z}_N$$

This operator gives the remainder on dividing $z = (x \times y)$ with N.

$$(6 \times 7) \pmod 5 \quad = 42 \pmod 5 \quad = 2 \in \mathbb{Z}_5$$

$$(62 \times 50) \pmod 7$$

bsdqm9

University of Kent

Modular Multiplication

We define

$$(x \times y) \pmod{N} =$$

$$z \pmod{N} = \underline{r} \in \mathbb{Z}_N$$

remainder

This operator gives the remainder on dividing $z = (x \times y)$ with N.

$$(6 \times 7) \pmod 5 = 42 \pmod 5 = 2 \in \mathbb{Z}_5$$

$$(62 \times 50) \pmod 7 = 3100 \pmod 7$$

Modular Multiplication

We define

$$(x \times y) \pmod N =$$

$$z \pmod N = \underline{r} \in \mathbb{Z}_N$$

remainder

This operator gives the remainder on dividing $z = (x \times y)$ with N.

$$(6 \times 7) \pmod 5 \quad = 42 \pmod 5 \quad = 2 \in \mathbb{Z}_5$$

$$(62 \times 50) \pmod 7 \quad = 3100 \pmod 7 \quad = 6 \in \mathbb{Z}_7$$

Modular Multiplication in $\mathbb{Z}_5$

For any two integers x and y,

$$x \times y \pmod{5} \in \{0, 1, 2, 3, 4\}.$$

Modular Multiplication in $\mathbb{Z}_5$

For any two integers x and y,

$$x \times y \pmod 5 \in \{0, 1, 2, 3, 4\}.$$

The following table shows the results of multiplications $\pmod 5$ of all elements of $\mathbb{Z}_5$ with each other.

Modular Multiplication in $\mathbb{Z}_5$

For any two integers x and y,

$$x \times y \pmod 5 \in \{0, 1, 2, 3, 4\}.$$

The following table shows the results of multiplications $\pmod 5$ of all elements of $\mathbb{Z}_5$ with each other.

Multiplication $\pmod 5$ in $\mathbb{Z}_5$

	0	1	2	3	4
0	0	0	0	0	0
1	0	1	2	3	4
2	0	2	4	1	3
3	0	3	1	4	2
4	0	4	3	2	1

Outline

Outline

bsdqm9

University of Kent

Prime Numbers

Definition:

A positive integer p is prime if it is only divisible by 1 and p.

Prime Numbers

Definition:

A positive integer p is prime if it is only divisible by 1 and p.

Some prime numbers:

- 2,

Prime Numbers

Definition:

A positive integer p is prime if it is only divisible by 1 and p.

Some prime numbers:

- $2, 3,$

Prime Numbers

Definition:

A positive integer p is prime if it is only divisible by 1 and p.

Some prime numbers:

- $2, 3, 5,$

Prime Numbers

Definition:

A positive integer p is prime if it is only divisible by 1 and p.

Some prime numbers:

- $2, 3, 5, 7,$

Prime Numbers

Definition:

A positive integer p is prime if it is only divisible by 1 and p.

Some prime numbers:

- $2, 3, 5, 7, 11,$

bsdqm9

Prime Numbers

Definition:

A positive integer p is prime if it is only divisible by 1 and p.

Some prime numbers:

- $2, 3, 5, 7, 11, 13,$

Prime Numbers

Definition:

A positive integer p is prime if it is only divisible by 1 and p.

Some prime numbers:

- $2, 3, 5, 7, 11, 13, 17,$

Prime Numbers

Definition:

A positive integer p is prime if it is only divisible by 1 and p.

Some prime numbers:

- $2, 3, 5, 7, 11, 13, 17, 19,$

bsdqm9

University of Kent

Prime Numbers

Definition:

A positive integer p is prime if it is only divisible by 1 and p.

Some prime numbers:

- $2, 3, 5, 7, 11, 13, 17, 19, 23, \ldots$

Prime Numbers

Definition:

A positive integer p is prime if it is only divisible by 1 and p.

Some prime numbers:

- $2, 3, 5, 7, 11, 13, 17, 19, 23, \ldots$

Algorithm: Check if n is prime or composite

Prime Numbers

Definition:

A positive integer p is prime if it is only divisible by 1 and p.

Some prime numbers:

- $2, 3, 5, 7, 11, 13, 17, 19, 23, \ldots$

Algorithm: Check if n is prime or composite

- For each divisor $2 \leq d \leq \sqrt{n}$: {

Prime Numbers

Definition:

A positive integer p is prime if it is only divisible by 1 and p.

Some prime numbers:

- $2, 3, 5, 7, 11, 13, 17, 19, 23, \ldots$

Algorithm: Check if n is prime or composite

- For each divisor $2 \leq d \leq \sqrt{n}$: {
  - If $n \mod d = 0$, then n is not a prime: {
    - hence, break the loop.

    }

  }

Prime Numbers

Definition:

A positive integer p is prime if it is only divisible by 1 and p.

Some prime numbers:

- $2, 3, 5, 7, 11, 13, 17, 19, 23, \ldots$

Algorithm: Check if n is prime or composite

- For each divisor $2 \leq d \leq \sqrt{n}$: {
  - If $n \mod d = 0$, then n is not a prime: {
    - hence, break the loop.

    }

  }
- If the above loop was not broken, then n is prime, else it is composite.

Note: $\sqrt{n}$ is a positive number such that $(\sqrt{n})^2 = n$

Prime Numbers

Is 56 a prime number?

Prime Numbers

Is 56 a prime number?

No, $d = 2$

Prime Numbers

Is 56 a prime number?

No, $d = 2$

Is 57 a prime number?

bsdqm9

Prime Numbers

Is 56 a prime number?

No, $d = 2$

Is 57 a prime number?

No, $d = 3$

bsdqm9

Prime Numbers

Is 56 a prime number?

No, $d = 2$

Is 57 a prime number?

No, $d = 3$

Is 59 a prime number?

bsdqm9

University of Kent

Prime Numbers

Is 56 a prime number?

No, $d = 2$

Is 57 a prime number?

No, $d = 3$

Is 59 a prime number?

Yes

bsdqm9 University of Kent

Prime Factorisation

Definition:

The prime factorisation of a positive integer n is defined as

$$n = p_1^{\alpha_1} \times p_2^{\alpha_2} \times \ldots \times p_k^{\alpha_k}$$

where

- $p_1, \ldots, p_k$ are prime numbers and
- $\alpha_1, \ldots, \alpha_k$ are positive integers

Prime Factorisation

Definition:

The prime factorisation of a positive integer n is defined as

$$n = p_1^{\alpha_1} \times p_2^{\alpha_2} \times \ldots \times p_k^{\alpha_k}$$

where

- $p_1, \ldots, p_k$ are prime numbers and
- $\alpha_1, \ldots, \alpha_k$ are positive integers

Examples:

2 =

bsdqm9

University of Kent

Prime Factorisation

Definition:

The prime factorisation of a positive integer n is defined as

$$n = p_1^{\alpha_1} \times p_2^{\alpha_2} \times \ldots \times p_k^{\alpha_k}$$

where

- $p_1, \ldots, p_k$ are prime numbers and
- $\alpha_1, \ldots, \alpha_k$ are positive integers

Examples:

$2 = 2^1$

$13 =$

Prime Factorisation

Definition:

The prime factorisation of a positive integer n is defined as

$$n = p_1^{\alpha_1} \times p_2^{\alpha_2} \times \ldots \times p_k^{\alpha_k}$$

where

- $p_1, \ldots, p_k$ are prime numbers and
- $\alpha_1, \ldots, \alpha_k$ are positive integers

Examples:

$2 = 2^1$

$13 = 2^0 \times 3^0 \times 5^0 \times 7^0 \times 11^0 \times 13^1 = 13^1$

$26 =$

bsdqm9

University of Kent

Prime Factorisation

Definition:

The prime factorisation of a positive integer n is defined as

$$n = p_1^{\alpha_1} \times p_2^{\alpha_2} \times \ldots \times p_k^{\alpha_k}$$

where

- $p_1, \ldots, p_k$ are prime numbers and
- $\alpha_1, \ldots, \alpha_k$ are positive integers

Examples:

2	$= 2^1$
13	$= 2^0 \times 3^0 \times 5^0 \times 7^0 \times 11^0 \times 13^1 = 13^1$
26	$= 2^1 \times 3^0 \times 5^0 \times 7^0 \times 11^0 \times 13^1 = 2^1 \times 13^1$
3468	$= ?$

Prime Factorisation: Algorithm

Algorithm to find $n = p_1^{\alpha_1} \times p_2^{\alpha_2} \times \ldots \times p_k^{\alpha_k}$:

- $n_1 \leftarrow n$
- For each step i, choose a prime $p_i \leq n_i$
  - Divide n_i with p_i as many times as possible to find α_i
  - Find n_{i+1} as:

$$n_{i+1} \leftarrow \frac{n_i}{p_i^{\alpha_i}}$$

bsdqm9

University of Kent

Prime Factorisation: Algorithm

Algorithm to find $n = p_1^{\alpha_1} \times p_2^{\alpha_2} \times \ldots \times p_k^{\alpha_k}$:

- $n_1 \leftarrow n$
- For each step i, choose a prime $p_i \leq n_i$
  - Divide n_i with p_i as many times as possible to find α_i
  - Find n_{i+1} as:

$$n_{i+1} \leftarrow \frac{n_i}{p_i^{\alpha_i}}$$

Example:

n_i	p_i	α_i	n_{i+1}

Prime Factorisation: Algorithm

Algorithm to find $n = p_1^{\alpha_1} \times p_2^{\alpha_2} \times \ldots \times p_k^{\alpha_k}$:

- $n_1 \leftarrow n$
- For each step i, choose a prime $p_i \leq n_i$
  - Divide n_i with p_i as many times as possible to find α_i
  - Find n_{i+1} as:

$$n_{i+1} \leftarrow \frac{n_i}{p_i^{\alpha_i}}$$

Example:

n_i	p_i	α_i	n_{i+1}
$n_1 = 3468$	$p_1 = 2$	$\alpha_1 =$	

Prime Factorisation: Algorithm

Algorithm to find $n = p_1^{\alpha_1} \times p_2^{\alpha_2} \times \ldots \times p_k^{\alpha_k}$:

- $n_1 \leftarrow n$
- For each step i, choose a prime $p_i \leq n_i$
  - Divide n_i with p_i as many times as possible to find α_i
  - Find n_{i+1} as:

$$n_{i+1} \leftarrow \frac{n_i}{p_i^{\alpha_i}}$$

Example:

n_i	p_i	α_i		n_{i+1}
$n_1 = 3468$	$p_1 = 2$	$\alpha_1 = 2$	$3468 = 2^2 \times 867$	$n_2 = 867$

Prime Factorisation: Algorithm

Algorithm to find $n = p_1^{\alpha_1} \times p_2^{\alpha_2} \times \ldots \times p_k^{\alpha_k}$:

- $n_1 \leftarrow n$
- For each step i, choose a prime $p_i \leq n_i$
  - Divide n_i with p_i as many times as possible to find α_i
  - Find n_{i+1} as:

$$n_{i+1} \leftarrow \frac{n_i}{p_i^{\alpha_i}}$$

Example:

n_i	p_i	α_i		n_{i+1}
$n_1 = 3468$	$p_1 = 2$	$\alpha_1 = 2$	$3468 = 2^2 \times 867$	$n_2 = 867$
$n_2 = 867$	$p_2 = 3$	$\alpha_2 =$		

Prime Factorisation: Algorithm

Algorithm to find $n = p_1^{\alpha_1} \times p_2^{\alpha_2} \times \ldots \times p_k^{\alpha_k}$:

- $n_1 \leftarrow n$
- For each step i, choose a prime $p_i \leq n_i$
  - Divide n_i with p_i as many times as possible to find α_i
  - Find n_{i+1} as:

$$n_{i+1} \leftarrow \frac{n_i}{p_i^{\alpha_i}}$$

Example:

n_i	p_i	α_i		n_{i+1}
$n_1 = 3468$	$p_1 = 2$	$\alpha_1 = 2$	$3468 = 2^2 \times 867$	$n_2 = 867$
$n_2 = 867$	$p_2 = 3$	$\alpha_2 = 1$	$867 = 3^1 \times 289$	$n_3 = 289$

bsdqm9

Prime Factorisation: Algorithm

Algorithm to find $n = p_1^{\alpha_1} \times p_2^{\alpha_2} \times \ldots \times p_k^{\alpha_k}$:

- $n_1 \leftarrow n$
- For each step i, choose a prime $p_i \leq n_i$
  - Divide n_i with p_i as many times as possible to find α_i
  - Find n_{i+1} as:

$$n_{i+1} \leftarrow \frac{n_i}{p_i^{\alpha_i}}$$

Example:

n_i	p_i	α_i		n_{i+1}
$n_1 = 3468$	$p_1 = 2$	$\alpha_1 = 2$	$3468 = 2^2 \times 867$	$n_2 = 867$
$n_2 = 867$	$p_2 = 3$	$\alpha_2 = 1$	$867 = 3^1 \times 289$	$n_3 = 289$
$n_3 = 289$	$p_3 = 5$	$\alpha_3 =$		

Prime Factorisation: Algorithm

Algorithm to find $n = p_1^{\alpha_1} \times p_2^{\alpha_2} \times \ldots \times p_k^{\alpha_k}$:

- $n_1 \leftarrow n$
- For each step i, choose a prime $p_i \leq n_i$
  - Divide n_i with p_i as many times as possible to find α_i
  - Find n_{i+1} as:

$$n_{i+1} \leftarrow \frac{n_i}{p_i^{\alpha_i}}$$

Example:

n_i	p_i	α_i		n_{i+1}
$n_1 = 3468$	$p_1 = 2$	$\alpha_1 = 2$	$3468 = 2^2 \times 867$	$n_2 = 867$
$n_2 = 867$	$p_2 = 3$	$\alpha_2 = 1$	$867 = 3^1 \times 289$	$n_3 = 289$
$n_3 = 289$	$p_3 = 5$	$\alpha_3 = 0$	$289 = 5^0 \times 289$	$n_4 = 289$

Prime Factorisation: Algorithm

Algorithm to find $n = p_1^{\alpha_1} \times p_2^{\alpha_2} \times \ldots \times p_k^{\alpha_k}$:

- $n_1 \leftarrow n$
- For each step i, choose a prime $p_i \leq n_i$
  - Divide n_i with p_i as many times as possible to find α_i
  - Find n_{i+1} as:

$$n_{i+1} \leftarrow \frac{n_i}{p_i^{\alpha_i}}$$

Example:

n_i	p_i	α_i		n_{i+1}
$n_1 = 3468$	$p_1 = 2$	$\alpha_1 = 2$	$3468 = 2^2 \times 867$	$n_2 = 867$
$n_2 = 867$	$p_2 = 3$	$\alpha_2 = 1$	$867 = 3^1 \times 289$	$n_3 = 289$
$n_3 = 289$	$p_3 = 5$	$\alpha_3 = 0$	$289 = 5^0 \times 289$	$n_4 = 289$
$n_4 = 289$	$p_4 = 7$	$\alpha_4 =$		

Prime Factorisation: Algorithm

Algorithm to find $n = p_1^{\alpha_1} \times p_2^{\alpha_2} \times \ldots \times p_k^{\alpha_k}$:

- $n_1 \leftarrow n$
- For each step i, choose a prime $p_i \leq n_i$
  - Divide n_i with p_i as many times as possible to find α_i
  - Find n_{i+1} as:

$$n_{i+1} \leftarrow \frac{n_i}{p_i^{\alpha_i}}$$

Example:

n_i	p_i	α_i		n_{i+1}
$n_1 = 3468$	$p_1 = 2$	$\alpha_1 = 2$	$3468 = 2^2 \times 867$	$n_2 = 867$
$n_2 = 867$	$p_2 = 3$	$\alpha_2 = 1$	$867 = 3^1 \times 289$	$n_3 = 289$
$n_3 = 289$	$p_3 = 5$	$\alpha_3 = 0$	$289 = 5^0 \times 289$	$n_4 = 289$
$n_4 = 289$	$p_4 = 7$	$\alpha_4 = 0$	$289 = 7^0 \times 289$	$n_5 = 289$

Prime Factorisation: Algorithm

Algorithm to find $n = p_1^{\alpha_1} \times p_2^{\alpha_2} \times \ldots \times p_k^{\alpha_k}$:

- $n_1 \leftarrow n$
- For each step i, choose a prime $p_i \leq n_i$
  - Divide n_i with p_i as many times as possible to find α_i
  - Find n_{i+1} as:

$$n_{i+1} \leftarrow \frac{n_i}{p_i^{\alpha_i}}$$

Example:

n_i	p_i	α_i		n_{i+1}
$n_1 = 3468$	$p_1 = 2$	$\alpha_1 = 2$	$3468 = 2^2 \times 867$	$n_2 = 867$
$n_2 = 867$	$p_2 = 3$	$\alpha_2 = 1$	$867 = 3^1 \times 289$	$n_3 = 289$
$n_3 = 289$	$p_3 = 5$	$\alpha_3 = 0$	$289 = 5^0 \times 289$	$n_4 = 289$
$n_4 = 289$	$p_4 = 7$	$\alpha_4 = 0$	$289 = 7^0 \times 289$	$n_5 = 289$
$n_5 = 289$	$p_5 = 11$	$\alpha_5 =$		

Prime Factorisation: Algorithm

Algorithm to find $n = p_1^{\alpha_1} \times p_2^{\alpha_2} \times \ldots \times p_k^{\alpha_k}$:

- $n_1 \leftarrow n$
- For each step i, choose a prime $p_i \leq n_i$
  - Divide n_i with p_i as many times as possible to find α_i
  - Find n_{i+1} as:

$$n_{i+1} \leftarrow \frac{n_i}{p_i^{\alpha_i}}$$

Example:

n_i	p_i	α_i		n_{i+1}
$n_1 = 3468$	$p_1 = 2$	$\alpha_1 = 2$	$3468 = 2^2 \times 867$	$n_2 = 867$
$n_2 = 867$	$p_2 = 3$	$\alpha_2 = 1$	$867 = 3^1 \times 289$	$n_3 = 289$
$n_3 = 289$	$p_3 = 5$	$\alpha_3 = 0$	$289 = 5^0 \times 289$	$n_4 = 289$
$n_4 = 289$	$p_4 = 7$	$\alpha_4 = 0$	$289 = 7^0 \times 289$	$n_5 = 289$
$n_5 = 289$	$p_5 = 11$	$\alpha_5 = 0$	$289 = 11^0 \times 289$	$n_6 = 289$

Prime Factorisation: Algorithm

Algorithm to find $n = p_1^{\alpha_1} \times p_2^{\alpha_2} \times \ldots \times p_k^{\alpha_k}$:

- $n_1 \leftarrow n$
- For each step i, choose a prime $p_i \leq n_i$
  - Divide n_i with p_i as many times as possible to find α_i
  - Find n_{i+1} as:

$$n_{i+1} \leftarrow \frac{n_i}{p_i^{\alpha_i}}$$

Example:

n_i	p_i	α_i		n_{i+1}
$n_1 = 3468$	$p_1 = 2$	$\alpha_1 = 2$	$3468 = 2^2 \times 867$	$n_2 = 867$
$n_2 = 867$	$p_2 = 3$	$\alpha_2 = 1$	$867 = 3^1 \times 289$	$n_3 = 289$
$n_3 = 289$	$p_3 = 5$	$\alpha_3 = 0$	$289 = 5^0 \times 289$	$n_4 = 289$
$n_4 = 289$	$p_4 = 7$	$\alpha_4 = 0$	$289 = 7^0 \times 289$	$n_5 = 289$
$n_5 = 289$	$p_5 = 11$	$\alpha_5 = 0$	$289 = 11^0 \times 289$	$n_6 = 289$
$n_6 = 289$	$p_6 = 13$	$\alpha_6 =$		

bsdqm9

University of Kent

Prime Factorisation: Algorithm

Algorithm to find $n = p_1^{\alpha_1} \times p_2^{\alpha_2} \times \ldots \times p_k^{\alpha_k}$:

- $n_1 \leftarrow n$
- For each step i, choose a prime $p_i \leq n_i$
  - Divide n_i with p_i as many times as possible to find α_i
  - Find n_{i+1} as:

$$n_{i+1} \leftarrow \frac{n_i}{p_i^{\alpha_i}}$$

Example:

n_i	p_i	α_i		n_{i+1}
$n_1 = 3468$	$p_1 = 2$	$\alpha_1 = 2$	$3468 = 2^2 \times 867$	$n_2 = 867$
$n_2 = 867$	$p_2 = 3$	$\alpha_2 = 1$	$867 = 3^1 \times 289$	$n_3 = 289$
$n_3 = 289$	$p_3 = 5$	$\alpha_3 = 0$	$289 = 5^0 \times 289$	$n_4 = 289$
$n_4 = 289$	$p_4 = 7$	$\alpha_4 = 0$	$289 = 7^0 \times 289$	$n_5 = 289$
$n_5 = 289$	$p_5 = 11$	$\alpha_5 = 0$	$289 = 11^0 \times 289$	$n_6 = 289$
$n_6 = 289$	$p_6 = 13$	$\alpha_6 = 0$	$289 = 13^0 \times 289$	$n_7 = 289$

Prime Factorisation: Algorithm

Algorithm to find $n = p_1^{\alpha_1} \times p_2^{\alpha_2} \times \ldots \times p_k^{\alpha_k}$:

- $n_1 \leftarrow n$
- For each step i, choose a prime $p_i \leq n_i$
  - Divide n_i with p_i as many times as possible to find α_i
  - Find n_{i+1} as:

$$n_{i+1} \leftarrow \frac{n_i}{p_i^{\alpha_i}}$$

Example:

n_i	p_i	α_i		n_{i+1}
$n_1 = 3468$	$p_1 = 2$	$\alpha_1 = 2$	$3468 = 2^2 \times 867$	$n_2 = 867$
$n_2 = 867$	$p_2 = 3$	$\alpha_2 = 1$	$867 = 3^1 \times 289$	$n_3 = 289$
$n_3 = 289$	$p_3 = 5$	$\alpha_3 = 0$	$289 = 5^0 \times 289$	$n_4 = 289$
$n_4 = 289$	$p_4 = 7$	$\alpha_4 = 0$	$289 = 7^0 \times 289$	$n_5 = 289$
$n_5 = 289$	$p_5 = 11$	$\alpha_5 = 0$	$289 = 11^0 \times 289$	$n_6 = 289$
$n_6 = 289$	$p_6 = 13$	$\alpha_6 = 0$	$289 = 13^0 \times 289$	$n_7 = 289$
$n_7 = 289$	$p_7 = 17$	$\alpha_7 =$		

Prime Factorisation: Algorithm

Algorithm to find $n = p_1^{\alpha_1} \times p_2^{\alpha_2} \times \ldots \times p_k^{\alpha_k}$:

- $n_1 \leftarrow n$
- For each step i, choose a prime $p_i \leq n_i$
  - Divide n_i with p_i as many times as possible to find α_i
  - Find n_{i+1} as:

$$n_{i+1} \leftarrow \frac{n_i}{p_i^{\alpha_i}}$$

Example:

n_i	p_i	α_i		n_{i+1}
$n_1 = 3468$	$p_1 = 2$	$\alpha_1 = 2$	$3468 = 2^2 \times 867$	$n_2 = 867$
$n_2 = 867$	$p_2 = 3$	$\alpha_2 = 1$	$867 = 3^1 \times 289$	$n_3 = 289$
$n_3 = 289$	$p_3 = 5$	$\alpha_3 = 0$	$289 = 5^0 \times 289$	$n_4 = 289$
$n_4 = 289$	$p_4 = 7$	$\alpha_4 = 0$	$289 = 7^0 \times 289$	$n_5 = 289$
$n_5 = 289$	$p_5 = 11$	$\alpha_5 = 0$	$289 = 11^0 \times 289$	$n_6 = 289$
$n_6 = 289$	$p_6 = 13$	$\alpha_6 = 0$	$289 = 13^0 \times 289$	$n_7 = 289$
$n_7 = 289$	$p_7 = 17$	$\alpha_7 = 2$	$289 = 17^2 \times 1$	$n_8 = 1$

Prime Factorisation

$$n = p_1^{\alpha_1} \times p_2^{\alpha_2} \times \ldots \times p_k^{\alpha_k}$$

Algorithm output:

3468

Prime Factorisation

$$n = p_1^{\alpha_1} \times p_2^{\alpha_2} \times \ldots \times p_k^{\alpha_k}$$

Algorithm output:

$$3468 \quad = 2^2 \times 867$$

Prime Factorisation

$$n = p_1^{\alpha_1} \times p_2^{\alpha_2} \times \ldots \times p_k^{\alpha_k}$$

Algorithm output:

$$\begin{aligned} 3468 \quad &= 2^2 \times 867 \\ &= 2^2 \times 3^1 \times 289 \end{aligned}$$

Prime Factorisation

$$n = p_1^{\alpha_1} \times p_2^{\alpha_2} \times \ldots \times p_k^{\alpha_k}$$

Algorithm output:

$$\begin{aligned} 3468 \quad &= 2^2 \times 867 \\ &= 2^2 \times 3^1 \times 289 \\ &= 2^2 \times 3^1 \times 5^0 \times 289 \end{aligned}$$

Prime Factorisation

$$n = p_1^{\alpha_1} \times p_2^{\alpha_2} \times \ldots \times p_k^{\alpha_k}$$

Algorithm output:

$$\begin{aligned} 3468 \quad &= 2^2 \times 867 \\ &= 2^2 \times 3^1 \times 289 \\ &= 2^2 \times 3^1 \times 5^0 \times 289 \\ &= 2^2 \times 3^1 \times 5^0 \times 7^0 \times 289 \end{aligned}$$

bsdqm9

University of Kent

Prime Factorisation

$$n = p_1^{\alpha_1} \times p_2^{\alpha_2} \times \ldots \times p_k^{\alpha_k}$$

Algorithm output:

$$\begin{aligned}
3468 \quad &= 2^2 \times 867 \\
&= 2^2 \times 3^1 \times 289 \\
&= 2^2 \times 3^1 \times 5^0 \times 289 \\
&= 2^2 \times 3^1 \times 5^0 \times 7^0 \times 289 \\
&= 2^2 \times 3^1 \times 5^0 \times 7^0 \times 11^0 \times 289
\end{aligned}$$

Prime Factorisation

$$n = p_1^{\alpha_1} \times p_2^{\alpha_2} \times \ldots \times p_k^{\alpha_k}$$

Algorithm output:

$$\begin{aligned}
3468 \quad &= 2^2 \times 867 \\
&= 2^2 \times 3^1 \times 289 \\
&= 2^2 \times 3^1 \times 5^0 \times 289 \\
&= 2^2 \times 3^1 \times 5^0 \times 7^0 \times 289 \\
&= 2^2 \times 3^1 \times 5^0 \times 7^0 \times 11^0 \times 289 \\
&= 2^2 \times 3^1 \times 5^0 \times 7^0 \times 11^0 \times 13^0 \times 289
\end{aligned}$$

We omit the primes with exponent 0 to write it in compact form:

$$3468 = 2^2 \times 3^1 \times 17^2.$$

Outline

LCM and GCD

Let a, b be positive integers such that

$$a = p_1^{\alpha_1} p_2^{\alpha_2} \dots p_k^{\alpha_k}, \alpha_i \geq 0$$

and

$$b = p_1^{\beta_1} p_2^{\beta_2} \dots p_k^{\beta_k}, \beta_i \geq 0$$

LCM and GCD

Let a, b be positive integers such that

$$a = p_1^{\alpha_1} p_2^{\alpha_2} \dots p_k^{\alpha_k}, \alpha_i \geq 0$$

and

$$b = p_1^{\beta_1} p_2^{\beta_2} \dots p_k^{\beta_k}, \beta_i \geq 0$$

Then,

$$lcm(a, b) =$$

LCM and GCD

Let a, b be positive integers such that

$$a = p_1^{\alpha_1} p_2^{\alpha_2} \dots p_k^{\alpha_k}, \alpha_i \geq 0$$

and

$$b = p_1^{\beta_1} p_2^{\beta_2} \dots p_k^{\beta_k}, \beta_i \geq 0$$

Then,

$$lcm(a, b) = p_1^{\max(\alpha_1, \beta_1)} p_2^{\max(\alpha_2, \beta_2)} \dots p_k^{\max(\alpha_k, \beta_k)}$$

LCM and GCD

Let a, b be positive integers such that

$$a = p_1^{\alpha_1} p_2^{\alpha_2} \dots p_k^{\alpha_k}, \alpha_i \geq 0$$

and

$$b = p_1^{\beta_1} p_2^{\beta_2} \dots p_k^{\beta_k}, \beta_i \geq 0$$

Then,

$$lcm(a, b) = p_1^{\max(\alpha_1, \beta_1)} p_2^{\max(\alpha_2, \beta_2)} \dots p_k^{\max(\alpha_k, \beta_k)}$$

and

$$gcd(a, b) =$$

LCM and GCD

Let a, b be positive integers such that

$$a = p_1^{\alpha_1} p_2^{\alpha_2} \ldots p_k^{\alpha_k}, \alpha_i \geq 0$$

and

$$b = p_1^{\beta_1} p_2^{\beta_2} \ldots p_k^{\beta_k}, \beta_i \geq 0$$

Then,

$$lcm(a, b) = p_1^{\max(\alpha_1, \beta_1)} p_2^{\max(\alpha_2, \beta_2)} \ldots p_k^{\max(\alpha_k, \beta_k)}$$

and

$$gcd(a, b) = p_1^{\min(\alpha_1, \beta_1)} p_2^{\min(\alpha_2, \beta_2)} \ldots p_k^{\min(\alpha_k, \beta_k)}.$$

Lowest Common Multiple (LCM)

Definition

For positive integers a, b, it is the smallest positive integer that is divisible by both a and b.

Lowest Common Multiple (LCM)

Definition

For positive integers a, b, it is the smallest positive integer that is divisible by both a and b.

Algorithm:

Lowest Common Multiple (LCM)

Definition

For positive integers a, b, it is the smallest positive integer that is divisible by both a and b.

Algorithm:

- Find the prime factorisation of both a and b

Lowest Common Multiple (LCM)

Definition

For positive integers a, b, it is the smallest positive integer that is divisible by both a and b.

Algorithm:

- Find the prime factorisation of both a and b
- $$lcm(a, b) = p_1^{\max(\alpha_1, \beta_1)} p_2^{\max(\alpha_2, \beta_2)} \ldots p_k^{\max(\alpha_k, \beta_k)}$$

Example: $lcm(20, 12)$

Lowest Common Multiple (LCM)

Definition

For positive integers a, b, it is the smallest positive integer that is divisible by both a and b.

Algorithm:

- Find the prime factorisation of both a and b
- $$lcm(a, b) = p_1^{\max(\alpha_1, \beta_1)} p_2^{\max(\alpha_2, \beta_2)} \cdots p_k^{\max(\alpha_k, \beta_k)}$$

Example: $lcm(20, 12)$

- $12 = 2^2 \times 3^1$

Lowest Common Multiple (LCM)

Definition

For positive integers a, b, it is the smallest positive integer that is divisible by both a and b.

Algorithm:

- Find the prime factorisation of both a and b
- $$lcm(a, b) = p_1^{\max(\alpha_1,\beta_1)} p_2^{\max(\alpha_2,\beta_2)} \cdots p_k^{\max(\alpha_k,\beta_k)}$$

Example: $lcm(20, 12)$

- $12 = 2^2 \times 3^1$
- $20 = 2^2 \times 5^1$

Lowest Common Multiple (LCM)

Definition

For positive integers a, b, it is the smallest positive integer that is divisible by both a and b.

Algorithm:

- Find the prime factorisation of both a and b
- $$lcm(a, b) = p_1^{\max(\alpha_1, \beta_1)} p_2^{\max(\alpha_2, \beta_2)} \dots p_k^{\max(\alpha_k, \beta_k)}$$

Example: $lcm(20, 12)$

- $12 = 2^2 \times 3^1$
- $20 = 2^2 \times 5^1$
- $lcm(20, 12) = 2^{\max(2,2)} \times 3^{\max(1,0)} \times 5^{\max(0,1)}$

Lowest Common Multiple (LCM)

Definition

For positive integers a, b, it is the smallest positive integer that is divisible by both a and b.

Algorithm:

- Find the prime factorisation of both a and b
- $$lcm(a, b) = p_1^{\max(\alpha_1, \beta_1)} p_2^{\max(\alpha_2, \beta_2)} \dots p_k^{\max(\alpha_k, \beta_k)}$$

Example: $lcm(20, 12)$

- $12 = 2^2 \times 3^1$
- $20 = 2^2 \times 5^1$
- $lcm(20, 12) = 2^{\max(2,2)} \times 3^{\max(1,0)} \times 5^{\max(0,1)} = 2^2 \times 3^1 \times 5^1 = 60$

Greatest Common Divisor (GCD)

Definition

For positive integers a, b, it is the largest positive integer that divides both a and b.

Greatest Common Divisor (GCD)

Definition

For positive integers a, b, it is the largest positive integer that divides both a and b.

Algorithm:

Greatest Common Divisor (GCD)

Definition

For positive integers a, b, it is the largest positive integer that divides both a and b.

Algorithm:

- Find the prime factorisation of both a and b

Greatest Common Divisor (GCD)

Definition

For positive integers a, b, it is the largest positive integer that divides both a and b.

Algorithm:

- Find the prime factorisation of both a and b
- $$gcd(a,b) = p_1^{\min(\alpha_1,\beta_1)} p_2^{\min(\alpha_2,\beta_2)} \cdots p_k^{\min(\alpha_k,\beta_k)}.$$

Example: $\gcd(20, 12)$

Greatest Common Divisor (GCD)

Definition

For positive integers a, b, it is the largest positive integer that divides both a and b.

Algorithm:

- Find the prime factorisation of both a and b
- $$gcd(a, b) = p_1^{\min(\alpha_1, \beta_1)} p_2^{\min(\alpha_2, \beta_2)} \cdots p_k^{\min(\alpha_k, \beta_k)}.$$

Example: $\gcd(20, 12)$

- $12 = 2^2 \times 3^1$

Greatest Common Divisor (GCD)

Definition

For positive integers a, b, it is the largest positive integer that divides both a and b.

Algorithm:

- Find the prime factorisation of both a and b
- $$gcd(a,b) = p_1^{\min(\alpha_1,\beta_1)} p_2^{\min(\alpha_2,\beta_2)} \dots p_k^{\min(\alpha_k,\beta_k)}.$$

Example: $\gcd(20, 12)$

- $12 = 2^2 \times 3^1$
- $20 = 2^2 \times 5^1$

Greatest Common Divisor (GCD)

Definition

For positive integers a, b, it is the largest positive integer that divides both a and b.

Algorithm:

- Find the prime factorisation of both a and b
- $$gcd(a, b) = p_1^{\min(\alpha_1,\beta_1)} p_2^{\min(\alpha_2,\beta_2)} \cdots p_k^{\min(\alpha_k,\beta_k)}.$$

Example: $\mathrm{gcd}(20, 12)$

- $12 = 2^2 \times 3^1$
- $20 = 2^2 \times 5^1$
- $\mathrm{gcd}(20, 12) = 2^{\min(2,2)} \times 3^{\min(1,0)} \times 5^{\min(0,1)}$

Greatest Common Divisor (GCD)

Definition

For positive integers a, b, it is the largest positive integer that divides both a and b.

Algorithm:

- Find the prime factorisation of both a and b
- $$gcd(a, b) = p_1^{\min(\alpha_1,\beta_1)} p_2^{\min(\alpha_2,\beta_2)} \cdots p_k^{\min(\alpha_k,\beta_k)}.$$

Example: $\gcd(20, 12)$

- $12 = 2^2 \times 3^1$
- $20 = 2^2 \times 5^1$
- $\gcd(20, 12) = 2^{\min(2,2)} \times 3^{\min(1,0)} \times 5^{\min(0,1)} = 2^2 \times 3^0 \times 5^0 = 4$

Outline

University of Kent

Two Theorems

Theorem 1

For any positive integer $n \neq 0$, n divides 0 and hence

$$\gcd(n, 0) = n.$$

Note: $n \times 0 = 0$.

Theorem 2

For positive integers a and $b \neq 0$,

$$\gcd(a, b) = \gcd(b, a \mod b).$$

Note: In $a = qb + r$, if d divides a and b, it will divide r as well.

The Euclidean Algorithm

Let $a \mod b$ be the remainder when a is divided by b.

The Euclidean Algorithm

Let $a \mod b$ be the remainder when a is divided by b.

Algorithm:

Keep using the fact (from Theorem 2) that, for $b \neq 0$, $\gcd(a, b) = \gcd(b, a \mod b)$ until $a \mod b = 0$.

The Euclidean Algorithm

Let $a \mod b$ be the remainder when a is divided by b.

Algorithm:

Keep using the fact (from Theorem 2) that, for $b \neq 0$, $\gcd(a, b) = \gcd(b, a \mod b)$ until $a \mod b = 0$.

Example: $\gcd(20, 12)$

$\gcd(20, 12) \quad =$

The Euclidean Algorithm

Let $a \mod b$ be the remainder when a is divided by b.

Algorithm:

Keep using the fact (from Theorem 2) that, for $b \neq 0$, $\gcd(a, b) = \gcd(b, a \mod b)$ until $a \mod b = 0$.

Example: $\gcd(20, 12)$

$$\begin{aligned} \gcd(20, 12) &= \gcd(12, 20 \mod 12) \\ &= \end{aligned}$$

The Euclidean Algorithm

Let $a \mod b$ be the remainder when a is divided by b.

Algorithm:

Keep using the fact (from Theorem 2) that, for $b \neq 0$, $\gcd(a, b) = \gcd(b, a \mod b)$ until $a \mod b = 0$.

Example: $\gcd(20, 12)$

$$\begin{aligned} \gcd(20, 12) &= \gcd(12, 20 \mod 12) \\ &= \gcd(12, 8) \\ &= \end{aligned}$$

bsdqm9

The Euclidean Algorithm

Let $a \mod b$ be the remainder when a is divided by b.

Algorithm:

Keep using the fact (from Theorem 2) that, for $b \neq 0$, $\gcd(a, b) = \gcd(b, a \mod b)$ until $a \mod b = 0$.

Example: $\gcd(20, 12)$

$$\begin{aligned}
\gcd(20, 12) &= \gcd(12, 20 \mod 12) \\
&= \gcd(12, 8) \\
&= \gcd(8, 12 \mod 8) \\
&=
\end{aligned}$$

The Euclidean Algorithm

Let $a \mod b$ be the remainder when a is divided by b.

Algorithm:

Keep using the fact (from Theorem 2) that, for $b \neq 0$, $\gcd(a, b) = \gcd(b, a \mod b)$ until $a \mod b = 0$.

Example: $\gcd(20, 12)$

$$\begin{aligned}
\gcd(20, 12) &= \gcd(12, 20 \mod 12) \\
&= \gcd(12, 8) \\
&= \gcd(8, 12 \mod 8) \\
&= \gcd(8, 4) \\
&=
\end{aligned}$$

The Euclidean Algorithm

Let $a \mod b$ be the remainder when a is divided by b.

Algorithm:

Keep using the fact (from Theorem 2) that, for $b \neq 0$, $\gcd(a, b) = \gcd(b, a \mod b)$ until $a \mod b = 0$.

Example: $\gcd(20, 12)$

$$\begin{aligned}
\gcd(20, 12) &= \gcd(12, 20 \mod 12) \\
&= \gcd(12, 8) \\
&= \gcd(8, 12 \mod 8) \\
&= \gcd(8, 4) \\
&= \gcd(4, 8 \mod 4) \\
&=
\end{aligned}$$

The Euclidean Algorithm

Let $a \mod b$ be the remainder when a is divided by b.

Algorithm:

Keep using the fact (from Theorem 2) that, for $b \neq 0$, $\gcd(a, b) = \gcd(b, a \mod b)$ until $a \mod b = 0$.

Example: $\gcd(20, 12)$

$$
\begin{aligned}
\gcd(20, 12) &= \gcd(12, 20 \mod 12) \\
&= \gcd(12, 8) \\
&= \gcd(8, 12 \mod 8) \\
&= \gcd(8, 4) \\
&= \gcd(4, 8 \mod 4) \\
&= \gcd(4, 0) \\
&=
\end{aligned}
$$

The Euclidean Algorithm

Let $a \mod b$ be the remainder when a is divided by b.

Algorithm:

Keep using the fact (from Theorem 2) that, for $b \neq 0$, $\gcd(a, b) = \gcd(b, a \mod b)$ until $a \mod b = 0$.

Example: $\gcd(20, 12)$

$$
\begin{aligned}
\gcd(20, 12) &= \gcd(12, 20 \mod 12) \\
&= \gcd(12, 8) \\
&= \gcd(8, 12 \mod 8) \\
&= \gcd(8, 4) \\
&= \gcd(4, 8 \mod 4) \\
&= \gcd(4, 0) \\
&= 4
\end{aligned}
$$

The Euclidean Algorithm

Another example: $\gcd(1734, 204)$

$$\gcd(1734, 204) \quad =$$

bsdqm9

University of Kent

The Euclidean Algorithm

Another example: $\gcd(1734, 204)$

$$\begin{aligned} \gcd(1734, 204) &= \gcd(204, 1734 \mod 204) \\ &= \end{aligned}$$

The Euclidean Algorithm

Another example: $\gcd(1734, 204)$

$$\begin{aligned}\gcd(1734, 204) &= \gcd(204, 1734 \mod 204) \\ &= \gcd(204, 102) \\ &= \end{aligned}$$

The Euclidean Algorithm

Another example: $\gcd(1734, 204)$

$$\begin{aligned} \gcd(1734, 204) &= \gcd(204, 1734 \mod 204) \\ &= \gcd(204, 102) \\ &= \gcd(102, 204 \mod 102) \\ &= \end{aligned}$$

The Euclidean Algorithm

Another example: $\gcd(1734, 204)$

$$\begin{aligned}
\gcd(1734, 204) &= \gcd(204, 1734 \mod 204)\\
&= \gcd(204, 102)\\
&= \gcd(102, 204 \mod 102)\\
&= \gcd(102, 0)\\
&=
\end{aligned}$$

bsdqm9

University of Kent

The Euclidean Algorithm

Another example: $\gcd(1734, 204)$

$$\begin{aligned}
\gcd(1734, 204) &= \gcd(204, 1734 \mod 204) \\
&= \gcd(204, 102) \\
&= \gcd(102, 204 \mod 102) \\
&= \gcd(102, 0) \\
&= 102
\end{aligned}$$

The Euclidean Algorithm: Advantages

Prime factorisation is costly!!!

So, finding LCM and GCD through prime factorisation will be inefficient.

The Euclidean Algorithm: Advantages

Prime factorisation is costly!!!

So, finding LCM and GCD through prime factorisation will be inefficient.

Example: $gcd(1734, 204)$

- Prime factorisation of 1734 would require

The Euclidean Algorithm: Advantages

Prime factorisation is costly!!!

So, finding LCM and GCD through prime factorisation will be inefficient.

Example: $gcd(1734, 204)$

- Prime factorisation of 1734 would require division by all $2 \leq d \leq \sqrt{1734}$

bsdqm9

University of Kent

The Euclidean Algorithm: Advantages

Prime factorisation is costly!!!

So, finding LCM and GCD through prime factorisation will be inefficient.

Example: $gcd(1734, 204)$

- Prime factorisation of 1734 would require division by all $2 \leq d \leq \sqrt{1734}$ (which are around 40 numbers)
- Prime factorisation of 204 would require

The Euclidean Algorithm: Advantages

Prime factorisation is costly!!!

So, finding LCM and GCD through prime factorisation will be inefficient.

Example: $gcd(1734, 204)$

- Prime factorisation of 1734 would require division by all $2 \leq d \leq \sqrt{1734}$ (which are around 40 numbers)
- Prime factorisation of 204 would require division by all $2 \leq d \leq \sqrt{204}$

The Euclidean Algorithm: Advantages

Prime factorisation is costly!!!

So, finding LCM and GCD through prime factorisation will be inefficient.

Example: $gcd(1734, 204)$

- Prime factorisation of 1734 would require division by all $2 \leq d \leq \sqrt{1734}$ (which are around 40 numbers)
- Prime factorisation of 204 would require division by all $2 \leq d \leq \sqrt{204}$ (which are around 14 numbers)
- Finally, the minimum exponents for each p_i have to be used to find the GCD

The Euclidean Algorithm: Advantages

Prime factorisation is costly!!!

So, finding LCM and GCD through prime factorisation will be inefficient.

Example: $gcd(1734, 204)$

- Prime factorisation of 1734 would require division by all $2 \leq d \leq \sqrt{1734}$ (which are around 40 numbers)
- Prime factorisation of 204 would require division by all $2 \leq d \leq \sqrt{204}$ (which are around 14 numbers)
- Finally, the minimum exponents for each p_i have to be used to find the GCD

The Euclidean algorithm requires at most 5 “such steps”!
It is much more efficient than the prime factorisation method!

Outline

bsdqm9

University of Kent

Mutually Prime

Definition

Two integers a and b are said to be mutually prime if there is no common factor between the two numbers other than 1.

Mutually Prime

Definition

Two integers a and b are said to be mutually prime if there is no common factor between the two numbers other than 1.

Alternate form

Two integers a and b are said to be mutually prime if $\gcd(a, b) = 1$.

Example: Mutually Prime

Are 14 and 21 mutually prime?

Example: Mutually Prime

Are 14 and 21 mutually prime?

$\gcd(14, 21) = 7$ which is > 1.
So, they are not mutually prime.

Example: Mutually Prime

Are 14 and 21 mutually prime?

$\gcd(14, 21) = 7$ which is > 1.
So, they are not mutually prime.

Are 110 and 273 mutually prime?

Example: Mutually Prime

Are 14 and 21 mutually prime?

$\gcd(14, 21) = 7$ which is > 1.
So, they are not mutually prime.

Are 110 and 273 mutually prime?

$\gcd(273, 110)$

Example: Mutually Prime

Are 14 and 21 mutually prime?

$\gcd(14, 21) = 7$ which is > 1.
So, they are not mutually prime.

Are 110 and 273 mutually prime?

$$\gcd(273, 110) = \gcd(110, 273 \mod 110)$$

Example: Mutually Prime

Are 14 and 21 mutually prime?

$\gcd(14, 21) = 7$ which is > 1.
So, they are not mutually prime.

Are 110 and 273 mutually prime?

$$\begin{aligned} \gcd(273, 110) &= \gcd(110, 273 \mod 110) \\ &= \gcd(110, 53) \end{aligned}$$

Example: Mutually Prime

Are 14 and 21 mutually prime?

$\gcd(14, 21) = 7$ which is > 1.
So, they are not mutually prime.

Are 110 and 273 mutually prime?

$$\begin{aligned}\gcd(273, 110) &= \gcd(110, 273 \mod 110)\\ &= \gcd(110, 53)\\ &= \gcd(53, 110 \mod 53)\end{aligned}$$

Example: Mutually Prime

Are 14 and 21 mutually prime?

$\gcd(14, 21) = 7$ which is > 1.
So, they are not mutually prime.

Are 110 and 273 mutually prime?

$$\begin{aligned}
\gcd(273, 110) &= \gcd(110, 273 \mod 110) \\
&= \gcd(110, 53) \\
&= \gcd(53, 110 \mod 53) \\
&= \gcd(53, 4)
\end{aligned}$$

Example: Mutually Prime

Are 14 and 21 mutually prime?

$\gcd(14, 21) = 7$ which is > 1.
So, they are not mutually prime.

Are 110 and 273 mutually prime?

$$\begin{aligned}
\gcd(273, 110) &= \gcd(110, 273 \mod 110) \\
&= \gcd(110, 53) \\
&= \gcd(53, 110 \mod 53) \\
&= \gcd(53, 4) \\
&= \gcd(4, 53 \mod 4)
\end{aligned}$$

Example: Mutually Prime

Are 14 and 21 mutually prime?

$\gcd(14, 21) = 7$ which is > 1.
So, they are not mutually prime.

Are 110 and 273 mutually prime?

$$
\begin{aligned}
\gcd(273, 110) &= \gcd(110, 273 \mod 110) \\
&= \gcd(110, 53) \\
&= \gcd(53, 110 \mod 53) \\
&= \gcd(53, 4) \\
&= \gcd(4, 53 \mod 4) \\
&= \gcd(4, 1)
\end{aligned}
$$

Example: Mutually Prime

Are 14 and 21 mutually prime?

$\gcd(14, 21) = 7$ which is > 1.
So, they are not mutually prime.

Are 110 and 273 mutually prime?

$$\begin{aligned}
\gcd(273, 110) &= \gcd(110, 273 \mod 110) \\
&= \gcd(110, 53) \\
&= \gcd(53, 110 \mod 53) \\
&= \gcd(53, 4) \\
&= \gcd(4, 53 \mod 4) \\
&= \gcd(4, 1) \\
&= \gcd(1, 4 \mod 1)
\end{aligned}$$

bsdqm9

Example: Mutually Prime

Are 14 and 21 mutually prime?

$\gcd(14, 21) = 7$ which is > 1.
So, they are not mutually prime.

Are 110 and 273 mutually prime?

$$\begin{aligned}
\gcd(273, 110) &= \gcd(110, 273 \mod 110) \\
&= \gcd(110, 53) \\
&= \gcd(53, 110 \mod 53) \\
&= \gcd(53, 4) \\
&= \gcd(4, 53 \mod 4) \\
&= \gcd(4, 1) \\
&= \gcd(1, 4 \mod 1) \\
&= \gcd(1, 0)
\end{aligned}$$

Example: Mutually Prime

Are 14 and 21 mutually prime?

$\gcd(14, 21) = 7$ which is > 1.
So, they are not mutually prime.

Are 110 and 273 mutually prime?

$$
\begin{aligned}
\gcd(273, 110) &= \gcd(110, 273 \mod 110) \\
&= \gcd(110, 53) \\
&= \gcd(53, 110 \mod 53) \\
&= \gcd(53, 4) \\
&= \gcd(4, 53 \mod 4) \\
&= \gcd(4, 1) \\
&= \gcd(1, 4 \mod 1) \\
&= \gcd(1, 0) \\
&= 1
\end{aligned}
$$

So, they are mutually prime.

Outline

Euler's phi function: $\phi(n)$

Definition

Let n be a positive integer.

Euler's phi function: $\phi(n)$

Definition

Let n be a positive integer. We define $\phi(n)$ as the number of integers between 1 and n that are mutually prime to n.

Find the value of $\phi(16)$

$n < 16$	$\gcd(16, n)$
1	

Find the value of $\phi(16)$

$n < 16$	$\gcd(16, n)$
1	1
2	

Find the value of $\phi(16)$

$n < 16$	$\gcd(16, n)$
1	1
2	2
3	

Find the value of $\phi(16)$

$n < 16$	$\gcd(16, n)$
1	1
2	2
3	1
4	

bsdqm9

University of Kent

Find the value of $\phi(16)$

$n < 16$	$\gcd(16, n)$
1	1
2	2
3	1
4	4
5	

Find the value of $\phi(16)$

$n < 16$	$\gcd(16, n)$
1	1
2	2
3	1
4	4
5	1
6	

Find the value of $\phi(16)$

$n < 16$	$\gcd(16, n)$
1	1
2	2
3	1
4	4
5	1
6	2
7	

bsdqm9

University of Kent

Find the value of $\phi(16)$

$n < 16$	$\gcd(16, n)$
1	1
2	2
3	1
4	4
5	1
6	2
7	1
8	

Find the value of $\phi(16)$

$n < 16$	$\gcd(16, n)$
1	1
2	2
3	1
4	4
5	1
6	2
7	1
8	8
9	

Find the value of $\phi(16)$

$n < 16$	$\gcd(16, n)$
1	1
2	2
3	1
4	4
5	1
6	2
7	1
8	8
9	1
10	

Find the value of $\phi(16)$

$n < 16$	$\gcd(16, n)$
1	1
2	2
3	1
4	4
5	1
6	2
7	1
8	8
9	1
10	2
11	

Find the value of $\phi(16)$

$n < 16$	$\gcd(16, n)$
1	1
2	2
3	1
4	4
5	1
6	2
7	1
8	8
9	1
10	2
11	1
12	

Find the value of $\phi(16)$

$n < 16$	$\gcd(16, n)$
1	1
2	2
3	1
4	4
5	1
6	2
7	1
8	8
9	1
10	2
11	1
12	4
13	

Find the value of $\phi(16)$

$n < 16$	$\gcd(16, n)$
1	1
2	2
3	1
4	4
5	1
6	2
7	1
8	8
9	1
10	2
11	1
12	4
13	1
14	

Find the value of $\phi(16)$

$n < 16$	$\gcd(16, n)$
1	1
2	2
3	1
4	4
5	1
6	2
7	1
8	8
9	1
10	2
11	1
12	4
13	1
14	2
15	

Find the value of $\phi(16)$

$n < 16$	$\gcd(16, n)$
1	1
2	2
3	1
4	4
5	1
6	2
7	1
8	8
9	1
10	2
11	1
12	4
13	1
14	2
15	1

So, $\phi(16) = 8$.

bsdqm9

Find the value of $\phi(16)$

$n < 16$	$\gcd(16, n)$
1	1
2	2
3	1
4	4
5	1
6	2
7	1
8	8
9	1
10	2
11	1
12	4
13	1
14	2
15	1

So, $\phi(16) = 8$.

This is a naive enumeration technique, and is costly!!!
We have a very smart mathematical way!

Euler's phi function: $\phi(n)$

Another way for finding the value of $\phi(n)$:

bsdqm9

University of Kent

Euler's phi function: $\phi(n)$

Another way for finding the value of $\phi(n)$:

1. Find the prime factorisation of n:

$$n = p_1^{\alpha_1} \times p_2^{\alpha_2} \times \ldots \times p_k^{\alpha_k}$$

Euler's phi function: $\phi(n)$

Another way for finding the value of $\phi(n)$:

1. Find the prime factorisation of n:

$$n = p_1^{\alpha_1} \times p_2^{\alpha_2} \times \ldots \times p_k^{\alpha_k}$$

2. Use the following formula

$$\phi(n) = n \prod_{i=1}^{k} \left(1 - \frac{1}{p_i}\right)$$

   This formula can be proved using the principle of inclusion-exclusion.

Find the value of $\phi(100)$

Find the value of $\phi(100)$

We know $100 = 2^2 \times 5^2$

Find the value of $\phi(100)$

We know $100 = 2^2 \times 5^2$

$$\begin{aligned}
\phi(100) &= 100 \prod_{i=1}^{2} \left(1 - \frac{1}{p_i}\right) \\
&= 100 \left(1 - \frac{1}{2}\right) \left(1 - \frac{1}{5}\right) \\
&= 100 \left(\frac{1}{2}\right) \left(\frac{4}{5}\right) \\
&= 40.
\end{aligned}$$

bsdqm9

University of Kent

Summary

Modular Arithmetic

- $+ \pmod{N}$ and $\times \pmod{N}$

Prime Factorisation

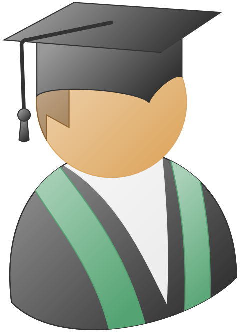
- Decompose an integer into prime numbers
- LCM is found by considering the maximum of the two exponents for a prime
- GCD is found by considering the minimum of the two exponents for a prime

Euclidean Algorithm

- A very efficient way to find GCD, without computing the prime factorisations

Mutually Prime Numbers

- When they have no common factors > 1
- In other words, when their GCD is 1



Thank you for your kind attention!