Introduction to Proofs - Number Theory
GCD and LCM

Prof Mike Pawliuk

UTM

August 13, 2020

Slides available at: mikepawliuk.ca

Learning Objectives (for this video)

By the end of this video, participants should be able to:

1. Relate GCD and LCM to the prime decomposition of a number.

Motivation

Motivation

Number theory is concerned with the divisors of natural numbers. Two numbers a and b are considered to be not similar (from a number theoretic perspective) if they share no common divisors, except 1.

In this video we will explore the definitions, and in the next video we will see a fast way for computing common factors.

Definition (GCD and LCM)

Let a, b be natural numbers.

1. The greatest common divisor (GCD) of a and b is the largest natural number n such that $n \mid a$ and $n \mid b$. It is denoted $\gcd(a, b)$.
2. The least common multiple (LCM) of a and b is the smallest natural number n such that $a \mid n$ and $b \mid n$. It is denoted $\text{lcm}(a, b)$.

Note that the definition of GCD and LCM also make sense if a, b are integers (not both 0).

a	b	$\gcd(a, b)$	$\text{lcm}(a, b)$	ab
4	6			
12	18			
1	20			

Definition (GCD and LCM)

Let a, b be natural numbers.

1. The greatest common divisor (GCD) of a and b is the largest natural number n such that $n \mid a$ and $n \mid b$. It is denoted $\gcd(a, b)$.
2. The least common multiple (LCM) of a and b is the smallest natural number n such that $a \mid n$ and $b \mid n$. It is denoted $\text{lcm}(a, b)$.

Note that the definition of GCD and LCM also make sense if a, b are integers (not both 0).

a	b	$\gcd(a, b)$	$\text{lcm}(a, b)$	ab
4	6	2	12	
12	18			
1	20			

Definition (GCD and LCM)

Let a, b be natural numbers.

1. The greatest common divisor (GCD) of a and b is the largest natural number n such that $n \mid a$ and $n \mid b$. It is denoted $\gcd(a, b)$.
2. The least common multiple (LCM) of a and b is the smallest natural number n such that $a \mid n$ and $b \mid n$. It is denoted $\text{lcm}(a, b)$.

Note that the definition of GCD and LCM also make sense if a, b are integers (not both 0).

a	b	$\gcd(a, b)$	$\text{lcm}(a, b)$	ab
4	6	2	12	
12	18	6	36	
1	20			

Definition (GCD and LCM)

Let a, b be natural numbers.

1. The greatest common divisor (GCD) of a and b is the largest natural number n such that $n \mid a$ and $n \mid b$. It is denoted $\gcd(a, b)$.
2. The least common multiple (LCM) of a and b is the smallest natural number n such that $a \mid n$ and $b \mid n$. It is denoted $\text{lcm}(a, b)$.

Note that the definition of GCD and LCM also make sense if a, b are integers (not both 0).

a	b	$\gcd(a, b)$	$\text{lcm}(a, b)$	ab
4	6	2	12	
12	18	6	36	
1	20	1	20	

Definition (GCD and LCM)

Let a, b be natural numbers.

1. The greatest common divisor (GCD) of a and b is the largest natural number n such that $n \mid a$ and $n \mid b$. It is denoted $\gcd(a, b)$.
2. The least common multiple (LCM) of a and b is the smallest natural number n such that $a \mid n$ and $b \mid n$. It is denoted $\text{lcm}(a, b)$.

Note that the definition of GCD and LCM also make sense if a, b are integers (not both 0).

a	b	$\gcd(a, b)$	$\text{lcm}(a, b)$	ab
4	6	2	12	24
12	18	6	36	216
1	20	1	20	20

2. Observations

Propositions

Let a, b be natural numbers.

1. $\gcd(a, b) \leq \text{lcm}(a, b)$.
2. $\gcd(a, b) \cdot \text{lcm}(a, b) = ab$.
3. $\gcd(a, b) \leq a, b \leq \text{lcm}(a, b)$.

3. Prime factorization is useful

Major idea

If the numbers a, b are given to us as products of primes, then computing the GCD and LCM is easy.

3. Prime factorization is useful

Major idea

If the numbers a, b are given to us as products of primes, then computing the GCD and LCM is easy.

Example

$\gcd(2^5, 2^7) =$

3. Prime factorization is useful

Major idea

If the numbers a, b are given to us as products of primes, then computing the GCD and LCM is easy.

Example

$\gcd(2^5, 2^7) = 2^5$

3. Prime factorization is useful

Major idea

If the numbers a, b are given to us as products of primes, then computing the GCD and LCM is easy.

Example

$\gcd(2^5, 2^7) = 2^5$

Proposition

Let p be a prime. If $a = p^n$ and $b = p^m$, and N is the smaller of n and m, then $\gcd(a, b) = p^N$.

3. Prime factorization is useful

Application

This can be used to compute the GCD of two numbers in prime factorization (by taking the minimum power of each prime).

3. Prime factorization is useful

Application

This can be used to compute the GCD of two numbers in prime factorization (by taking the minimum power of each prime).

Example

$\gcd(2^6 3^8, 2^5 3^{10}) =$

3. Prime factorization is useful

Application

This can be used to compute the GCD of two numbers in prime factorization (by taking the minimum power of each prime).

Example

$\gcd(2^6 3^8, 2^5 3^{10}) = 2^5$

3. Prime factorization is useful

Application

This can be used to compute the GCD of two numbers in prime factorization (by taking the minimum power of each prime).

Example

$\gcd(2^6 3^8, 2^5 3^{10}) = 2^5 3^8$ (Check that this really does divide both!)

3. Prime factorization is useful

Application

This can be used to compute the GCD of two numbers in prime factorization (by taking the minimum power of each prime).

Example

$\gcd(2^6 3^8, 2^5 3^{10}) = 2^5 3^8$ (Check that this really does divide both!)

Exercise. Come up with a similar method for computing LCM of two numbers in prime factorization. Use this to prove that $ab = \gcd(a, b) \cdot \text{lcm}(a, b)$.

4. Converting to Prime factorization

Question

Is it easy to find the prime factors of a number?

4. Converting to Prime factorization

Question

Is it easy to find the prime factors of a number?

Former $75'000 exercise

Consider this number (called RSA-896) with 270 digits. This has exactly 2 prime factors.

$$
\begin{aligned}
&412023436986659543855531365332575948179811699844\\
&327982845455626433876445565248426198098870423161\\
&841879261420247188869492560931776375033421130982\\
&397485150944909106910269861031862704114880866970\\
&564902903653658867433731720813104105190864254793\\
&282601391257624033946373269391
\end{aligned}
$$

Reflection

- How can you find the gcd of two numbers?
- How can you (easily) find the lcm of two number if you are given their prime decompositions?
- Is it easy to find the prime decomposition of two numbers?
- What's the largest prime number you can find (including using software).