Number Theory:
Greatest Common Divisor & Least Common Multiple

Adila A. Krisnadhi

Fakultas Ilmu Komputer, Universitas Indonesia

Version date: 2022-02-16 05:05:25+07:00
Reference: Rosen, Ed.8, Ch.4

Motivating question

Jakarta's recent flood damaged Dobbie's room quite significantly. Before Dobbie can use his room again, he has to conduct some renovation work, which includes installing new tiles to the floor.

The room's shape is rectangular measuring 420 cm $\times$ 364 cm. Dobbie only wants square tiles and moreover, he wants as few tiles as possible such that the whole floor is perfectly covered only by square tiles, i.e., no non-square tile has to be used. Fortunately, one of Dobbie's business partners is a tile supplier that can provide him with square tiles of any size.

What is the minimum number of tiles do Dobbie actually use?

Greatest common divisor (GCD)

Definition (GCD)

Let a, b be integers, not both zero. The **greatest common divisor (GCD) of a and b**, denoted $\gcd(a, b)$, is the **largest** integer that divides both a and b, i.e., the largest integer d such that $d \mid a$ and $d \mid b$.

- $\gcd(36, 48) =$
- $\gcd(25, 21) =$

GCD and prime factorization

Write the prime factorization of:

- 36, 48, and $\gcd(36, 48)$
- 25, 21, and $\gcd(25, 21)$
- 120, 500, and $\gcd(120, 500)$.

Can you spot the pattern?

Let a, b be integers with $a \leqslant b$. Also, let $p_1, p_2, \ldots, p_n$ be primes such that for every p_i, $p_i \mid a$ or $p_i \mid b$. Then, prime factorizations of a and b can be written:

$$a = p_1^{a_1} p_2^{a_2} \cdots p_n^{a_n} \qquad b = p_1^{b_1} p_2^{b_2} \cdots p_n^{b_n}$$

where $a_1, \ldots, a_n, b_1, \ldots, b_n$ are nonnegative integers. Then, the following theorem holds.

Theorem (GCD and prime factorization)

$$\gcd(a, b) = p_1^{\min(a_1, b_1)} p_2^{\min(a_2, b_2)} \cdots p_n^{\min(a_n, b_n)}$$

Relatively prime

Definition

Two integers a and b are called **coprime** or **relatively prime** iff $\gcd(a, b) = 1$.

n integers $a_1, a_2, \ldots, a_n$ are **pairwise coprime** or **pairwise relatively prime** iff $\gcd(a_i, a_j) = 1$ for $1 \leqslant i < j \leqslant n$.

That is, two integers are coprime if their only common positive factor is 1.

- Are 10 and 21 relatively prime?
- Are 44, 50, and 63 pairwise relatively prime?
- Are 21, 25, and 56 pairwise relatively prime?

Least common multiple (LCM)

Definition

Least common multiple of a and b, denoted $\mathrm{lcm}(a, b)$, is the smallest positive integer that is divisible by both a and b.

What is $\mathrm{lcm}(95256, 432)$?

LCM and prime factorization

Can you express LCM using prime factorization?

LCM and prime factorization

Can you express LCM using prime factorization?
Write the prime factorization of 95256, 432, and their LCM. Guess the pattern.

Theorem

If a, b are integers with prime factorizations according to the theorem in Slide 5, then

$$\operatorname{lcm}(a,b) = p_1^{\max(a_1,b_1)} p_2^{\max(a_2,b_2)} \cdots p_n^{\max(a_n,b_n)}$$

Relationship between GCD and LCM

Is there a relation between GCD and LCM of two integers?

Relationship between GCD and LCM

Is there a relation between GCD and LCM of two integers?
Guess the relation by first calculating the following integers:

- 36, 48, $\gcd(36, 48)$, $\mathrm{lcm}(36, 48)$
- 25, 21, $\gcd(25, 21)$, $\mathrm{lcm}(25, 21)$
- 120, 500, $\gcd(120, 500)$, $\mathrm{lcm}(125, 500)$

Theorem

Let a, b be positive integers. Then, $ab = \gcd(a, b) \cdot \operatorname{lcm}(a, b)$

- $\gcd(95256, 432) =$
- $\operatorname{lcm}(36, 48) =$

Calculating GCD

- Based on what we've seen so far, how do we calculate the GCD of two integers?

Calculating GCD

- Based on what we've seen so far, how do we calculate the GCD of two integers?
  - Prime factorization

Calculating GCD

- Based on what we've seen so far, how do we calculate the GCD of two integers?
  - Prime factorization
- Is the above approach efficient?

Calculating GCD

- Based on what we've seen so far, how do we calculate the GCD of two integers?
  - Prime factorization
- Is the above approach efficient?
  - In current practice, no.
  - In theory, No polynomial-time algorithm for prime factorization of all integers has been found so far. Prime factorization is in class NP, but has not been shown to be NP-complete. It is suspected that the problem is neither in class P nor it is NP-complete.
  - **Note:** In 1994, Peter Shor found an algorithm for prime factorization that could be run in polynomial time on **quantum** computers.

Calculating GCD

- Based on what we've seen so far, how do we calculate the GCD of two integers?
  - Prime factorization
- Is the above approach efficient?
  - In current practice, no.
  - In theory, No polynomial-time algorithm for prime factorization of all integers has been found so far. Prime factorization is in class NP, but has not been shown to be NP-complete. It is suspected that the problem is neither in class P nor it is NP-complete.
  - **Note:** In 1994, Peter Shor found an algorithm for prime factorization that could be run in polynomial time on **quantum** computers.
- Is there an efficient way to calculate GCD?

Calculating GCD

- Based on what we've seen so far, how do we calculate the GCD of two integers?
  - Prime factorization
- Is the above approach efficient?
  - In current practice, no.
  - In theory, No polynomial-time algorithm for prime factorization of all integers has been found so far. Prime factorization is in class NP, but has not been shown to be NP-complete. It is suspected that the problem is neither in class P nor it is NP-complete.
  - **Note:** In 1994, Peter Shor found an algorithm for prime factorization that could be run in polynomial time on **quantum** computers.
- Is there an efficient way to calculate GCD?
  - Yes: the Euclidean algorithm.

Euclidean algorithm: the key idea

Let's compute $\gcd(21, 78)$. For this, consider the integers 78, 21, 15, 6, 3, 0.

- Calculate the GCD of every two consecutive integers using any means you know. Can you spot the pattern?
- Generalize it so that we consider $\gcd(a, b)$ for any integers a, b.

Theorem (Core of Euclidean algorithm)

Let a, b be integers. Then, $\gcd(a, b) = \gcd(b, a \bmod b)$

- $\gcd(21, 78) =$
- $\gcd(25, 21) =$

Proof of Theorem 7?

Algorithm (Euclidean algorithm to calculate $\gcd(a, b)$)

Input: a, b positive integers
$x \coloneqq a$
$y \coloneqq b$
while $y \neq 0$:
  $r \coloneqq x \bmod y$
  $x \coloneqq y$
  $y \coloneqq r$
return x $\rightsquigarrow$ x is $\gcd(a, b)$

Euclidean algorithm using tabulation

We use a table of values $r_j, r_{j+1}, q_{j+1}, r_{j+2}$ for $j = 0, 1, \ldots$ where

- $r_0 = a$, $r_1 = b$,
- $r_j = r_{j+1}q_{j+1} + r_{j+2}$ for j
- iteration is terminated at $j = n$ when $r_{j+2} = 0$ and $r_{j+1} = \gcd(a, b)$

Calculate $\gcd(662, 414)$ using tabulation: iterate on $j = 0, 1, \ldots$ with $r_0 = a$, $r_1 = b$, $r_j = r_{j+1}q_{j+1} + r_{j+2}$ for j, and terminate at $j = n$ when $r_{j+2} = 0$ dan $r_{j+1} = \gcd(a, b)$

$\gcd(a, b)$ as linear combination of a and b

- $\gcd(6, 14) = 2$ and $2 = (-2) \cdot 6 + 1 \cdot 14$
- $\gcd(25, 21) = 1$ and $1 = (-5) \cdot 25 + 6 \cdot 21$
- $\gcd(36, 48) = 12$ and $12 = (-1) \cdot 36 + 1 \cdot 48$

Does this hold in general? Given a and b, can we find the correct linear combination (on the right) for $\gcd(a, b)$?

Theorem (Bezout's Theorem)

Let a, b be integers. Then, there exists integers s and t such that $\gcd(a, b) = sa + tb$.

Note: s or t can be negative.

Two ways to calculate s and t above:

- Calculate the $\gcd$ using Euclidean algorithm, and then perform the reverse calculation.
- Direct calculation using the **extended Euclidean algoritm** $\rightsquigarrow$ Read Exercise 41 in Section 4.3.

Example

Express $\gcd(252, 198)$ as a linear combination of 252 and 198.