Greatest Common Divisors

Let a and b be integers, not both zero. The largest integer d such that d | a and d | b is called the **Greatest common divisor** of a and b.
The greatest common divisor of a and b is denoted by gcd(a, b).

Example 1: What is gcd(48, 72) ?
The positive common divisors of 48 and 72 are 1, 2, 3, 4, 6, 8, 12, 16, and 24, so gcd(48, 72) = 24.

Example 2: What is gcd(25, 15) ?
The only positive common divisor of 25 and 15 is 5, so gcd(25, 15) = 5.

Greatest Common Divisors

Using prime factorizations:

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

where $p_1 < p_2 < \ldots < p_n$ and $a_i, b_i \in \mathbf{N}$ for $1 \le i \le n$

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

Example:

$a = 60 = 2^2\ 3^1\ 5^1$

$b = 54 = 2^1\ 3^3\ 5^0$

$\gcd(a, b) = 2^1\ 3^1\ 5^0 = 6$

Relatively Prime Integers

Definition:
Two integers a and b are **relatively prime** if gcd(a, b) = 1.

Examples:
Are 15 and 28 relatively prime?
Yes, gcd(15, 28) = 1.

Are 55 and 28 relatively prime?
Yes, gcd(55, 28) = 1.

Are 35 and 28 relatively prime?
No, gcd(35, 28) = 7.

Relatively Prime Integers

The integers a_1 , $a_2, \ldots\ldots,$ a_n are *pairwise relatively prime* if gcd*(*a_i, a_j *)* = 1 whenever 1 ≤ *i* < *j* ≤ *n*.

Examples:

Are 15, 17, and 27 pairwise relatively prime?
No, because gcd(15, 27) = 3.

Are 15, 17, and 28 pairwise relatively prime?
Yes, because gcd(15, 17) = 1, gcd(15, 28) = 1 and gcd(17, 28) = 1.

Euclidean algorithm

Formal description of the Euclidean algorithm

- Input: Two positive integers, a and b.
- Output: The greatest common divisor of a and b.

- Internal computation

1. If a<b, exchange a and b.
2. Divide a by b and get the remainder r.
3. If r=0, report b as the GCD of a and b.
   Else replace a by b and replace b by r. Return to the previous step.

The Euclidean Algorithm

In pseudocode, the algorithm can be implemented as follows:

```
procedure gcd(a, b: positive integers)
x := a
y := b
while y ≠ 0
begin
        r := x mod y
        x := y
        y := r
end {x is gcd(a, b)}
```

The Euclidean algorithm is a way to find the greatest common divisor of two positive integers a and b. **GCD (a, b) = GCD (b, a mod b)**

Example 1: GCD (210,45)

1. 210 /45 = 4 with remainder r= 30, so $210=4\cdot45+30$.

2. 45 /30=1 with remainder r=15, so $45=1\cdot30+15$.

3. 30 / 15=2 with remainder r=0, so $30=2\cdot15+0$.

4. The greatest common divisor of 210 and 45 is 15.

Example 2

Gcd(27,18)

27= 18*1 +9

18= 9*2+0

Therefore: Gcd(27,18)=9

Example 3

Gcd(287,91)

287=91*3+14

91=14*6+7

14=7*2+0

Therefore: Gcd(287,91)=7

Least Common Multiples

Definition:

The **least common multiple** of the positive integers a and b is the smallest positive integer that is divisible by both a and b. We denote the least common multiple of a and b by lcm(a, b).

Examples:

lcm(3, 7) = 21

lcm(4, 6) = 12

lcm(5, 10) = 10

Least Common Multiples

Using prime factorizations:

$a = p_1^{a_1} \ p_2^{a_2} \ldots p_n^{a_n}$, $b = p_1^{b_1} \ p_2^{b_2} \ldots p_n^{b_n}$,
where $p_1 < p_2 < \ldots < p_n$ and $a_i, b_i \in \mathbf{N}$ for $1 \leq i \leq n$

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

Example:

$a = 60 = 2^2 \ 3^1 \ 5^1$

$b = 54 = 2^1 \ 3^3 \ 5^0$

$\mathrm{lcm}(a, b) = 2^2 \ 3^3 \ 5^1 = 4 \cdot 27 \cdot 5 = 540$

GCD and LCM

$a = 60 = 2^2 \; 3^1 \; 5^1$

$b = 54 = 2^1 \; 3^3 \; 5^0$

$\gcd(a, b) = 2^1 \; 3^1 \; 5^0 = 6$

$\text{lcm}(a, b) = 2^2 \; 3^3 \; 5^1 = 540$

Theorem: $a \cdot b = \gcd(a,b) \cdot \text{lcm}(a,b)$