Lecture 3: Greatest Common Divisors and Least Common Multiples

Greatest Common Divisor

Given two positive integers a and b, the **greatest common divisor (factor)** is the largest factor that divides both a and b. We use $\gcd(a, b)$ to denote the greatest common divisor (GCD).

Example

- If a divides b, then $\gcd(a, b) = a$.
  - $\gcd(3, 6) = 3$
  - $\gcd(12, 2) = 2$
- If p is a prime, then $\gcd(p, a) = 1 \text{ or } p$.
  - $\gcd(5, 16) = 1$
  - $\gcd(5, 100) = 5$
- $\gcd(a, b)$ is always less than a and b.
  - $\gcd(15, 24) = 3$
  - $\gcd(91, 52) = 13$

GCD from the prime factorization

Example

- Since $91 = 7 * 13$ and $52 = 2^2 * 13$, then GCD can be read directly from the common prime factors, in this case, it is 13.
- In general, once you know the prime factorization, just pick the common prime factors and the smaller exponent.
  - $$\gcd(2^2 * 3^3 * 5, 2^3 * 3^2 * 7) = 2^2 * 3^2 = 36$$
  - $$\gcd(2^{100} * 3^{40} * 13^2, 3^7 * 5^5 * 13) = 3^7 * 13$$
- If you already observe a common factor c, then

$$\gcd(a, b) = c \cdot \gcd(\frac{a}{b}, \frac{b}{c})$$

  - $\gcd(112, 80) = 4 * \gcd(28, 20) = 16$
  - $\gcd(126, 162) = 6 * \gcd(21, 27) = 18$

Warning: This is a really inefficient algorithm. In general, prime factorization is costly even for computers when the number is very large.

Homework Ask ChatGPT for a prime factorization algorithm and ask it to time the algorithm. Try a relatively large number about 10 digits for example.

Euclidean algorithm (300 BC)

The most efficient algorithm (Wiki link) to calculate $\gcd(a,b)$:

- Step 1: Assume a is the smaller number. Calculate b divided by a with the remaider r:

$$b = k \cdot a + r$$

- Step 2: If $r = 0$, then $\gcd(a,b) = a$. If $r \neq 0$, then $\gcd(a,b) = \gcd(a,r)$. Now repeat Step 1 on $\gcd(a,r)$.

Example

- $\gcd(80,112) = \gcd(80,32) = \gcd(16,32) = 16$
- $\gcd(105,252) = \gcd(105,42) = \gcd(21,42) = 21$
- $\gcd(162,126) = \gcd(36,126) = \gcd(36,18) = 18$
- $\gcd(80,112 + 80 * 123456789) = \gcd(80,112) = 16$
- $\gcd(1800000001,30) = 1$
- $\gcd(a,a+1) = 1$

We can define $\gcd(a,b,c)$.
Example Find a,b,c such that $\gcd(a,b,c) = 1$ but GCD of any two are not 1.
Solution: $\gcd(2*3, 3*5, 5*2) = 1$

Least common multiple

Given two positive integers a and b, the **least common multiple** is the smallest number that both a and b divides. We use $\operatorname{lcm}(a,b)$ to denote LCM. We always have

$$\operatorname{lcm}(a,b) \leq ab$$

Example

- $\operatorname{lcm}(4,6) = 12$
- $\operatorname{lcm}(12,16) = 48$
- If $\gcd(a,b) = 1$, in other words, no common factors, then $\operatorname{lcm}(a,b) = ab$.
  - $\operatorname{lcm}(4,13) = 52$

- $\operatorname{lcm}(a, a+1) = a(a+1)$
- If c divides both a and b, then

$$\operatorname{lcm}(a, b) = c \cdot \operatorname{lcm}(a/c, b/c)$$

LCM formula

LCM via prime factorization is quite easy.Take all prime factors and the higher exponents.

Example

- $\operatorname{lcm}(2^2, 2*3) = 2^2 * 3 = 12$
- $\operatorname{lcm}(2^2 * 3^3 * 5, 2*3*7) = 2^2 * 3^3 * 5 * 7$

We can use the following formula to calculate LCM in general.

$$\gcd(a, b)\operatorname{lcm}(a, b) = a \cdot b$$

Number Proof
If $a = 2^3 \cdot 3^5 \cdot 7 \cdot 17$ and $b = 2^2 \cdot 3^7 \cdot 7^2 \cdot 19$, then

$$\gcd(a, b) = 2^2 \cdot 3^5 \cdot 7$$

$$\operatorname{lcm}(a, b) = 2^3 \cdot 3^7 \cdot 7^2 \cdot 17 \cdot 19$$

You can verify this directly.

Proof We can pull out GCD as below.

$$\operatorname{lcm}(a, b) = \gcd(a, b)\operatorname{lcm}(\frac{a}{\gcd(a, b)}, \frac{b}{\gcd(a, b)})$$

Note that $\frac{a}{\gcd(a,b)}, \frac{b}{\gcd(a,b)}$ have no common GCD. Thus

$$\operatorname{lcm}(\frac{a}{\gcd(a, b)}, \frac{b}{\gcd(a, b)}) = \frac{a}{\gcd(a, b)} \cdot \frac{b}{\gcd(a, b)}$$

Plug this into the first equation. We are done.