CS 2050 Discrete Mathematics February 22nd 2024

Lecture 13: Greatest Common Divisor

Lecturer: Abrahim Ladha

1 GCD

Definition 1.1. For two numbers a, b the greatest common divisor of a, b is a number $d \geq 1$ such that $d \mid a$ and $d \mid b$.

gcd(a, b) computes the greatest common divisor of a, b. For example, $gcd(105, 30) = gcd(3 \cdot 5 \cdot 7, 2 \cdot 3 \cdot 5) = 3 \cdot 5 = 15$. You can analogously think of gcd like a set intersection. What number is greatest to divide into both a, b? If $a = 2^2$ and $b = 2^3$, then their greatest common divisor must be 2^2.

2 Euclidean Algorithm

The following is an easy divide and conquer algorithm discovered long ago by Euclid to calculate gcd of any two numbers.

```
function gcd(a, b)
if b = 0
    return a
else
    return gcd(b, a mod b)
```

Proof of Correctness: We can prove correctness by proving that $gcd(a, b) = gcd(a, a - b)$. Repeatedly subtracting b from a will give you $a \pmod b$. We will show these two numbers to be equal by proving that they divide each other. If two numbers divide each other, they must be equal, as a number is greater than or equal to any of its factors.

Proof. Let $d = gcd(a, b)$. If $d \mid a$ (d divides a), and $d \mid b$ (d divides b), then $a = dk$, and similarly $b = dl$ for some numbers k, l. So, $a - b = dk - dl = d(k - l)$. Therefore, d is a factor of $a - b$, hence $d \mid (a - b)$. So, $d \mid gcd(b, a - b)$.

Let $gcd(b, a - b) = d'$. Then, $d' \mid b$, $d' \mid (a - b)$. So $d' \mid (a - b) + b = a$. So $d' \mid a$ and $d' \mid b \implies d' \mid gcd(a, b) \implies d' = d$. Since these two numbers divide each other, they must be equal. Easy!! □

You can think of the euclidean algorithm as swapping (a, b) for a pair of smaller numbers with the same gcd.

$$gcd(25, 11) = gcd(11, 3) = gcd(3, 2) = gcd(2, 1) = gcd(1, 0) = 1$$

To write the execution of the algorithm, put the larger number on the left hand side, and represent it in division form $a = bq + r$. Then repeatedly chain down.

$$\begin{aligned}\gcd(25,11) &= \\ 25 &= 2\cdot 11+3 \\ 11 &= 3\cdot 3+2 \\ 3 &= 1\cdot 2+1 \\ 2 &= 2\cdot 1+0\end{aligned}$$

When the last remainder is zero, then you have your greatest common divisor.

3 Extended Euclidean Algorithm

Theorem 1 (Bezout's)**.** For any numbers a, b there exists integers s, t such that

$$gcd(a,b) = as + bt$$

Bezout's theorem is incredibly important, but we won't be able to prove it with the tools we have now. We will be able to show you how to calculate s, t given $a, b, \gcd(a,b)$. The calculation simply takes the execution of the euclidean algorithm, and uses it to find s, t. As we computed the euclidean algorithm, we went through a sequence of pairs

$$(25,11) \to (11,3) \to (3,2) \to (2,1) \to (1,0)$$

We will work backwards through the pairs, until we are left with a linear combination of the first pair. For example, we will replace 3 with a linear combination of 25 and 11. The way we will do this, is by taking the steps of the euclidean algorithm and substituting them back into each other back up until the first one. First, take your equations, and rewrite them with the remainder on one side

$$\begin{aligned}\gcd(25,11) &= & \\ 25 &= 2\cdot 11+3 & 3 &= 25(1)+11(-2) \\ 11 &= 3\cdot 3+2 & 2 &= 11(1)+3(-3) \\ 3 &= 1\cdot 2+1 & 1 &= 3(1)+2(-1) \\ 2 &= 2\cdot 1+0 & 0 &= 2(1)+2(-1)\end{aligned}$$

Our pairs are (1,0), (2,1), (3,2), (11,3) and (25,11). Let us compute s, t such that $25s + 11t = 1$ working backwards First, write the $gcd(a,b) = 1$ as a linear combination of the first pair, (1,0)

$$1 = 1 + 0$$

Next, we want to go from pair (1,0) to pair (2,1) so we will use the last equation of $0 = ...$ and substitute this in.

$$1 = 1 + \mathbf{0} = 1 + [2(1) + 2(-1)] = 2(-1) + 1(3)$$

Note how we have written the linear combination of (0,1) as a linear combination of (2,1). Let us substitute out the 1 for a linear combination of 3 and 2. Since we leave the 2 unchanged, we will have a linear combination of 3 and 2.

$$1 = 2(-1) + \mathbf{1}(3) = 2(-1) + [3(1) + 2(-1)](3) = 3(3) + 2(-4)$$

Now we replace the 2 with the linear combination of 11 and 3.

$$1 = 3(3) + \mathbf{2}(-4) = 3(3) + [11(1) + 3(-3)](-4) = 11(-4) + 3(15)$$

Replace 3 with a linear combination of 25 and 11 and we will be complete

$$11(-4) + \mathbf{3}(15) = 11(-4) + [25(1) + 11(-2)](15) = 25(15) + 11(-34)$$

So we may conclude that

$$1 = 25(15) + 11(-34)$$

For $a, b = 25, 11$ our values of $s, t = 15, -34$. These are not guaranteed to be unique or minimal, and you may find other numbers which work, but the extended Eucldean algorithm is guaranteed to give you a pair of numbers s, t to satisfy Bezout's theorem.

4 Fundamental Theorem of Arithmetic

Lets prove a theorem to make some proofs easier.

Theorem 2 (Fundamental Theorem of Arithmetic)**.** Every number has a unique prime factorization

Proof. Assume to the contrary a number has a non-unique prime factorization. $n = p_1...p_k = q_1...q_l$ where $p_1, ..., p_k, q_1, ..., q_k$ are all primes. By assumption to the contrary, there is some p_i not equal to any q_j for any j.

Since $p_i \mid n$, notice that $p_i \mid q_1...q_l$. Since p_i is prime, then $p_i \mid q_j$ for some q_j. Since q_j is prime, then it must be the case that not only $p_i \mid q_j$, but that $p_i = q_j$. Contradicting our assumption p_i is not equal to any q_j. □

5 LCM

Definition 5.1. For any two numbers a, b, the least common multiple of a, b is the smallest number l such that $a \mid l$ and $b \mid l$

One way to compute the lcm of two numbers is to write out two sequences of multiples of numbers, and take the first number to appear in both. For example, to compute that $lcm(4, 6) = 12$, you could observe that:

$$4, 8, 12, 16, ...$$
$$6, 12, ...$$

Is there a better way to compute the lcm? We give a relationship between lcm, gcd, and the product.

6 relationship LCM and GCD

Theorem 3. For any numbers $a, b \geq 1$ it is true that

$$\gcd(a,b)\text{lcm}(a,b) = ab$$

Proof. By the fundamental theorem of arithmetic, a, b have unique prime factorizations. Without loss of generality, suppose that a has p_k as its largest prime divisor and b has p_l as its largest prime divisor with $k \geq l$. Suppose the factorizations are

$$a = 2^{a_1}3^{a_2}...p_k^{a_k} = \prod_{i=1}^{k} p_i^{a_i}$$

$$b = 2^{b_1}3^{b_2}...p_l^{b_l} = \prod_{i=1}^{l} p_i^{b_i}$$

Since $\gcd(a,b) \mid a$ and $\gcd(a,b) \mid b$ we know that

$$\gcd(a,b) = 2^{\min(a_1,b_1)}3^{\min(a_2,b_2)} \cdot ... \cdot p_k^{\min(a_k,b_k)} = \prod_{i=1}^{k} p_i^{\min(a_i,b_i)}$$

Similarly, the least common multiple must be large enough to accomodate all the prime divisors of both a, b so

$$\text{lcm}(a,b) = 2^{\max(a_1,b_1)}3^{\max(a_2,b_2)} \cdot ... \cdot p_k^{\max(a_k,b_k)} = \prod_{i=1}^{k} p_i^{\max(a_i,b_i)}$$

Since $k \geq l$, the values for b_i with $i > l$ may be zero. Then

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

$$\Big(\prod_{i=1}^{k} p_i^{\min(a_i,b_i)}\Big) \cdot \Big(\prod_{i=1}^{k} p_i^{\max(a_i,b_i)}\Big) =$$

$$\Big(\prod_{i=1}^{k} p_i^{\min(a_i,b_i)+\max(a_i,b_i)}\Big)$$

For any two numbers, x, y it is true that $\max(x,y) + \min(x,y) = x + y$. One will be the min, the other must be the max. So

$$\Big(\prod_{i=1}^{k} p_i^{\min(a_i,b_i)+\max(a_i,b_i)}\Big) = \Big(\prod_{i=1}^{k} p_i^{a_i+b_i}\Big) =$$

$$\Big(\prod_{i=1}^{k} p_i^{a_i} p_i^{b_i}\Big) =$$

$$\Big(\prod_{i=1}^{k} p_i^{a_i}\Big) \cdot \Big(\prod_{i=1}^{k} p_i^{b_i}\Big) = ab$$

□