CS 30: Discrete Math in CS (Winter 2019): Lecture 8

Date: 16th January, 2019 (Wednesday)
Topic: GCD and Euclid's Algorithm
Disclaimer: These notes have not gone through scrutiny and in all probability contain errors.
Please discuss in Piazza/email errors to deeparnab@dartmouth.edu

---

1. **GCD and co-prime numbers.** The *greatest common divisor* $g = \gcd(a, b)$ of two positive integers a and b is the *largest* integer g such that g perfectly divides both a and b. That is, $g \equiv 0 \bmod a$ and $g \equiv 0 \bmod b$. Two numbers a and b are *relatively prime or co-prime* if $\gcd(a, b) = 1$.

2. **Key Property of GCD.**

   Theorem 1 (GCD property)**.** Given any two positive numbers a, b with say $b \leq a$, let r be the remainder upon dividing a by b. That is, $a = bq + r$ for some $0 \leq r < b$. If $r = 0$, then $\gcd(a, b) = b$. Otherwise, $\gcd(a, b) = \gcd(b, r)$.

   Proof. If $r = 0$ then b divides a, b clearly divides b, and there is no larger number that divides b. Thus, $\gcd(a, b) = b$.

   Otherwise, let $g = \gcd(a, b)$ and $h = \gcd(b, r)$. Since g divides a and g divides bq, we get g divides $r = a - bq$. Thus, $\gcd(b, r) \geq g$ since the GCD is the *largest* integer dividing both b and r. Since h divides b and h divides r, h divides $a = bq + r$. Thus, $\gcd(a, b) \geq h$. Thus, $g = h$. □

3. **Euclid's Recursive Algorithm for GCD.** The above fact can be used to obtain the GCD of a and b.

```
procedure GCD(a, b) ▷ Assume a ≥ b.
    ▷ Returns the GCD of a and b.
    Divide a by b to get a = bq + r.
    if r = 0 then:
        return b
    else:
        return GCD(b, r)
```

   Exercise: *Why does the above algorithm terminate?*

4. **Certificate of GCD.** Here is another way of looking at GCDs. $g = \gcd(a, b)$ is the *smallest positive* number g which can be expressed as an *integer combination* of a and b, that is, g can be written as $g = xa + yb$ where x and y are integers, and no smaller positive number can be expressed thus.

Theorem 2. For any two positive numbers a and b, the GCD $g := \gcd(a,b)$ is the *smallest, positive* integer which can be expressed as an *integer linear combination* of a and b. That is,

$$\gcd(a,b) = \min \ \{xa + yb : x \in \mathbb{Z}, \ \ y \in \mathbb{Z}, \ \text{ and } \ xa + yb > 0\} \tag{1}$$

Proof.

- One direction is easy. We first show that for any two integers x, y such that $xa + yb > 0$, we must have $xa + yb \geq g$. Indeed, let us call the number $xa + yb = n$. Since g divides both a and b, g must divide n. Thus, $n = gq$ for some integer q. However, $n > 0$ and $g > 0$, which implies $q > 0$. Since q is integer, we must have $q \geq 1$ implying $n = gq \geq g$.
- The more interesting direction is to show that there indeed exists integers x and y such that $xa + yb = g$. Indeed, for the sake of contradiction, suppose this is not the case. That is, there exist some "bad" pair of positive numbers a and b such that no matter which integers x and y we choose, $xa + yb \neq g$
- *Minimal Counterexample Idea.* Now we use another very nice proof idea which we will build upon a lot in a couple of weeks. Among all such "bad" pairs of numbers (a,b), let us pick the pair which has the *smallest sum* $(a+b)$. Why is this *well defined*? Well, for any bad pair the sum $a + b$ is a positive number (in fact ≥ 2); if we "sort" the bad pairs in increasing order of sum (breaking ties arbitrarily), then we pick the first such pair.
- Now, suppose $a \geq b$ (without loss of generality). Let (q,r) be such that $a = bq + r$ and $0 \leq r < b$. Note that if $r = 0$, then $\gcd(a,b) = b$ and $b = 0 \cdot a + 1 \cdot b$ implying (a,b) cannot be bad. So, $0 < r < b$.
- But this means (b,r) is a pair of positive integers with $b + r < b + a$. Since (a,b) was the *bad pair with the smallest sum*, the pair (b,r) *cannot be bad*; if it were, I would've picked (b,r) instead of (a,b). So (b,r) is *not bad*, which implies there *must exist* integers x', y' such that
$$x'b + y'r = \gcd(b,r) = \gcd(a,b)$$
where the last equality follows from Theorem 1.
- But then,
$$x'b + y'(a - bq) = g \quad \Rightarrow \quad y'a + (x' - y'q)b = g$$
that is, we have expressed g as an integer linear combination of a and b. This contradicts that (a,b) was a bad pair at all.

□

Remark: *The above gives a "short" certificate to prove a number $g = \gcd(a,b)$. Think for a minute what it takes to prove to some one g is the GCD of two numbers a and b. For instance, how can you prove that 44621 is the GCD of 2892199357 and 1499845673? Sure, we can check that g divides both a and b; but that only proves that the GCD is **greater than or equal to** g. How do we prove equality? If we were to do brute force, then we have to take **all** numbers bigger than g and check that none of them divide both a and b. This is rather time consuming.*

The above fact shows that a smaller proof would be to find the x and y such that $g = xa + yb$. This would then show that the GCD is less than or equal to g. *Combined with the above, it will show that g is indeed the GCD. For the above two numbers, for instance, we can see that* $44621 = 6544 \times 2892199357 + (-12619) \times 1499845673$ *proving that* 44621 *is indeed the GCD.*

5. **Extended Euclid Algorithm.** Indeed the above proof gives a *recursive* algorithm to find a pair of integers (x, y) such that $xa + yb = \gcd(a, b)$. This is given below.

```
procedure EXTGCD(a, b)  ▷ Assume a ≥ b ≥ 0.
    ▷ Returns the GCD of a and b. Also returns x, y such that xa + yb = gcd(a, b)
    Divide a by b to get a = bq + r.
    if r = 0 then:
        return (b, 0, 1)
    else:
        Let (g, x', y') = EXTGCD(b, r).
        return (g, y', x' − y'q)
```

Exercise: *Code the algorithm up in your favorite language.*

Exercise: *Are the x, y unique?. That is, can there be some other x', y' such that $x'a + y'b = \gcd(a, b)$?*

A useful corollary is the following. It is, for instance, useful to prove two numbers are relatively prime.

Theorem 3. If there exist integers x, y such that $xa + yn = 1$, then $\gcd(a, n) = 1$.

Exercise: *Prove that any two consecutive numbers are relatively prime.*

Exercise: *Prove that any two consecutive odd numbers are relative prime.*