Numbers: GCD and Bezout's Identity[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. Two numbers a and b are *relatively prime or co-prime* if $\gcd(a, b) = 1$.

  Examples:

  - $\gcd(5, 1) = 1$. If one of the numbers is 1, then the $\gcd$ must be 1. No number larger than 1 divides it. And 1 divides every number.
  - $\gcd(10, 5) = 5$. More generally, if b divides a, then $\gcd(a, b) = b$. Why? Well, definitely b divides both b and a. Can there by anything larger, say c, which divides b? No. Any number c that divides b *must* be $\leq b$.
  - $\gcd(13, 17) = 1$. In general, the $\gcd(p, q)$ of two primes is 1. This is from the *definition* of prime numbers. A number p is prime if 1 and p are its only factors.
  - $\gcd(12, 16) = 4$. The "grade school" way of showing this (at least if I remember my grade school) is to write $12 = 2 \times 2 \times 3$ and $16 = 2 \times 2 \times 2 \times 2$. And the $\gcd$ is the product of all the common things.

  Remark: *The above is a bad way to find, or even prove, GCDs because of two reasons which are worth comprehending.*

  a. *First, it assumes the* ***unique prime factorization theorem*** *of numbers. That is,* 12 *can be written as the product of* $2 \cdot 2 \cdot 3$*, and that there is* no other *way of doing so. Because, imagine if both* 12 *and* 16 *did have different ways of being written, and in one way* 8 *came out as a common divisor! Well one cannot quite assume the* unique *factorization theorem, for that actually needs stuff building on what we will do in class today (we won't cover unique factorization in this course though). So, using unique factorization is* circular.
  b. *Second, even if you assume unique factorization (which you cannot for reason mentioned above), we simply don't know how to* **factor** *numbers easily. Sure* 12 *and* 16 *are fine. But can you factor* 1194649 *in your head? Or a* 100 *digit number in your computer? We just don't know how!*

  So, the $\gcd$ concept is not as trivial. Given two numbers a and b, unless one divides the other, how do we actually find the $\gcd$? Today's class will tell us (a) a way to do so, and (b) also a quick way to *certify* a GCD. Certify as in the Prover-Verifier model we had talked about for bipartite graphs and L-matchings. All this is more than 2000 years old!!

- **Key Property of GCD.** Here is what Euclid noticed.

[1] *Lecture notes by Deeparnab Chakrabarty. Last modified : 28th Aug, 2021*
These have not gone through scrutiny and may contain errors. If you find any, or have any other comments, please email me at deeparnab@dartmouth.edu. Highly appreciated!

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. We already notices the $r = 0$ case. To repeat, 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 b, and therefore, 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, $g = h$. □

Example. So, using Theorem 1, we can make progress on $\gcd(16, 12)$. 12 doesn't divide 16, but rather $16 \bmod 12 = 4$. Thus, the above theorem gives us $\gcd(16, 12) = \gcd(12, 4)$. But now, 4 does divide 12, and so $\gcd(12, 4) = 4$. Indeed, $\gcd(16, 12) = 4$ (as our grade-school had predicted.)

- **Euclid's Recursive Algorithm for GCD.** Indeed, the above example is an illustration of a recursive algorithm to obtain the GCD of a and b.

```
procedure GCD($a, b$) ▷ Assume $a \geq b$.
    ▷ 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($b, r$)
```

Example. Let us run this with a different set of numbers; say 25 and 15.

GCD$(25, 15)$	$25 = 15 \cdot 1 + 10$	$q = 1, \quad r = 10$	calls
GCD$(15, 10)$	$15 = 10 \cdot 1 + 5$	$q = 1, \quad r = 5$	calls
GCD$(10, 5)$	$10 = 2 \cdot 5 + 0$	$q = 2, \quad r = 0$	recursion stops, returns 5.

Why does the above algorithm terminate? Well, in each recursive call, the *smaller* number passed on to GCD is strictly becoming smaller. Do you see why? Yes, because the remainder is always smaller than the divisor; $r < b$. Furthermore, when the smaller number becomes 1, we know that the algorithm will stop. So it will at least stop in some finite time.

In fact, the above algorithm is pretty darn fast. And we analyze it completely in CS31!

Exercise: *Code the above algorithm in your favorite language, and then pass on* 100 *digit numbers to it and marvel. PS: If you are using Python, set the max recursion depth limit though. If you don't know what that meant, Google it.*

- **Integer Linear Combinations and Bezout's Identity.** We now come to a quite fascinating identity which will form the heart of most things we are going to say in this module. It has all the characteristics of a beautiful theorem: it's surprising (at least it was to me), it's extremely useful (see the UGP, for instance), and actually simple to prove (we have already done almost all the work!).

  Before we dive into the identity, let's *play* a bit. Fix two natural numbers a and b. We then consider *all* numbers that can be obtained by taking *integer linear combinations* of these numbers. That is, we consider the set[2]

  $$L(a,b) := \{xa + yb : x \in \mathbb{Z}, y \in \mathbb{Z}\}$$

  We observe that any number $\ell \in L(a,b)$ must be *divisible* by $g = \gcd(a,b)$. Why? Well, simply because g divides both a and b. And thus, g divides $xa + yb$ for any two integers x and y. The question that probably arises in one is: are *all* multiples of g obtained? Clearly, the answer to this is equivalent to whether $g \in L(a,b)$? If $g \in L(a,b)$, that is, if $x^*a + y^*b = g$, then any multiple kg of g is also in $L(a,b)$ since $(kx^*)a + (ky^*)b = kg$. Is it possible $g \in L(a,b)$? The answer is YES! This is what is called Bezout's Identity (but Euclid knew of this too).

  Theorem 2. (Bezout's Identity)

  For any two positive numbers a and b, there exists two *integers* x and y (not necessarily positive) such that

  $$xa + yb = \gcd(a,b) \qquad \text{(Bezout's Identity)}$$

  Remark: *I say "not necessarily positive" above, however, they both* ***cannot*** *be positive. For then $xa + yb$ is bigger than both a and b, while $\gcd(a,b)$ is at most a or b.*

  In English, Bezout's identity says that given any two positive numbers a and b, there is a *integer linear combination* of these numbers to get the GCD of the pair. And thus the set $L(a,b)$ are simply the multiples of g. In particular, if a and b are relatively prime, then $L(a,b) = \mathbb{Z}$, all integers. Thus,

  Theorem 3. If a and b are relatively prime numbers, then for *any* integer z, there is a solution (x,z) to the equation $xa + yb = z$.

  Proof. Bezout's identity says there exists x^* and y^* such that $x^*a + y^*b = 1$. Multiply by z to get the solution $x = x^*z$ and $y = y^*z$. $\square$

  Before we go into the proof, let us see one application and one important corollary.

  Claim 1. If $g = \gcd(a,b)$ and h is a *common divisor* of a and b, then h divides g.

  Proof. Note the definition of g just implies $h \le g$. But Bezout's identity *immediately* implies this. Indeed, there is x, y with $xa + yb = g$. Since h divides a and b, it divides the LHS, and so h divides g. $\square$

[2] such a set formed by integer combinations are called a lattice. Hence the letter L

Theorem 4. Let a and b be two positive natural numbers. If there exist integers x, y such that $xa + yb = 1$, then $\gcd(a, b) = 1$. That is, a and b are relatively prime.

Proof. Let $g := \gcd(a, b)$. Then since g divides a and b, g divides $xa + yn$. But the only number which divides 1 is 1. Thus, $g = 1$. $\square$

Remark: *Using the Prover-Verifier analogy once more. Suppose I have two very large numbers a and b and the Prover tells me that they are relatively prime. They can now easily provide a* certificate *by giving an x and a y such that $xa + yb = 1$.*

For example, take $a = 234234534535$ and $b = 42371897123$. I can claim that they are relatively prime, by asserting

$$15306622845 \times a + (-84615981838) \times b = 1$$

And you can verify this even with a calculator. Do it!

Remark: *I also lost a lot of people on this theorem last time. So, pay attention, and ask questions.*

Argument. Before we embark on the formal proof, let us look at a very simple case: when one of the number divides the other. Suppose b divides a, and thus, $\gcd(a, b) = b$. Are there integers x, y such that $xa + yb = \gcd(a, b) = b$? Sure! Set $x = 0$ and set $y = 1$.

Ok, now suppose b *doesn't* divide a. Recall, this was precisely the case where we were "stuck" with gcd as well. So, $a = bq + r$ for some $0 < r < b$. Well, what does Theorem 1 tell us? It tells us $\gcd(a, b) = \gcd(b, r)$. Let's call this number g. But how does it help in finding the integers x and y such that $xa + yb = g$?

Here comes the key insight. The pair (b, r) is "simpler" than the pair (a, b). More precisely, the smaller number in the pair is strictly less. But their gcd's are the same. So? So, ***inductively***, *we can assume that there are integers u and v such that $ub + vr = \gcd(b, r) = g$.*

We wanted to write g as an integer combination of a and b. What we have achieved, by induction, is that we have written it as an integer combination of b and r. How is that useful? Well, what is r? r is *also* an integer combination of a and b's, right. After all, $a = bq + r$ which implies $r = a - bq$ (this was also used in Theorem 1 proof). And so, we can use this to write g as an integer combination of a's and b's.

More precisely,

$$g = ub + vr \quad \Rightarrow g = ub + v \cdot (a - bq) \quad \Rightarrow g = v \cdot a + (u - vq) \cdot b$$

To sum up, if we inductively/recursively solve the problem on (b, r) to write $g = \gcd(b, r)$ as a integer combination of b and r as $\gcd(b, r) = ub + vr$, then we can obtain an integer linear combination of $\gcd(a, b)$ as $xa + yb$ by setting $x = v$ and $y = u - vq$ where q was the quotient when a was divided by b.

Example. Let's take the numbers 25 and 15 for which we calculated the GCD of 5 above. We see that in Step 1, we wrote $25 = 15 \cdot 1 + 10$, so the quotient q was 1 whole remainder r was 10. So, this means if some one gave us a way to write $5 = \gcd(15, 10)$ as a linear combination of 15 and 10, and for instance one way is $5 = 15 \cdot 1 + 10 \cdot (-1)$ with $u = 1$ and $v = -1$, then one can write 5 as a integer combination of 25 and 15 by setting $x = v = -1$, and $y = (u - vq) = (1 - (-1) \cdot 1) = 2$; indeed,

$$5 = (-1) \cdot 25 + 2 \cdot 15$$

Let me give the exact recursive code below which encapsulates the above argument, then run with another example, then state a very important *corollary* of the theorem, and then finally give *two* (really the same) formal proofs of the theorem. But by now you should be able to formalize the proof as well.

```
procedure EXTGCD($a, b$) ▷ Assume $a \geq b \geq 0$.
    ▷ 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 $(g, u, v)$ =EXTGCD$(b, r)$.
        return $(g, v, u - vq)$
```

Example Run, and how to write on paper. Let us actually run this algorithm for $a = 17$ and $b = 12$.

EXTGCD$(17, 12)$		$17 = 12 \cdot 1 + 5$	$q_1 = 1, \ \ r_1 = 5$	calls
EXTGCD$(12, 5)$		$12 = 5 \cdot 2 + 1$	$q_2 = 2, \ \ r_2 = 2$	calls
EXTGCD$(5, 2)$		$5 = 2 \cdot 2 + 1$	$q_3 = 2, \ \ r_3 = 1$	calls
EXTGCD$(2, 1)$		$2 = 1 \cdot 2 + 0$	$r_4 = 0$ recursion stops	
EXTGCD$(2, 1)$	returns	$x_4 = 0, y_4 = 1, \mathbf{gcd} = \mathbf{1}$	*check:* $0 \cdot 2 + 1 \cdot 1 = 1$	
EXTGCD$(5, 2)$	returns	$x_3 = y_4 = 1, y_3 = (x_4 - y_4 q_3) = -2$	*check:* $1 \cdot 5 + (-2) \cdot 2 = 1$	
EXTGCD$(12, 5)$	returns	$x_2 = y_3 = -2, y_2 = (x_3 - y_3 q_2) = 5$	*check:* $(-2) \cdot 12 + 5 \cdot 5 = 1$	
EXTGCD$(17, 12)$	returns	$x_1 = y_2 = 5, y_1 = (x_2 - y_2 q_1) = -7$	*check:* $(5) \cdot 17 + (-7) \cdot 12 = 1$	

Thus the final answer is $(x_1, y_1, g) = (5, -7, 1)$.

- **Formal proofs of Theorem 2.**

Proof #1. We will actually prove the code EXTGCD works correctly (remember the lecture one proving recursive codes correct?) We define the following predicate:

For any natural number b, $P(b)$ is true if and only if for *all* pairs of natural numbers $a \geq b$ EXTGCD(a, b) returns (g, x, y) such that (a) $g = \gcd(a, b)$, and (b) $g = xa + yb$.

Now note that if we prove $\forall n \in \mathbb{N} : P(n)$ is true, then we would have proved the theorem. We proceed by induction.

Base Case: We first establish $P(1)$ is true. If $b = 1$, then note that for any $a \geq b$, b divides a. Thus, we run Line 5, that is, we return $(b, 0, 1) = (1, 0, 1)$. Indeed, the gcd is 1, and $1 = 0 \cdot a + 1 \cdot 1$. Therefore, the algorithm behaves correctly, and $P(1)$ is established.

Inductive Case: Now fix a natural number $k \geq 2$. Assume $P(2), P(3), \ldots, P(k)$ is true. We intend to show $P(k+1)$ is true. That is, for any number $a \geq (k+1)$, we intend to show that $\text{ExtGCD}(a, k+1)$ behaves correctly. To this end, fix a natural number $a \geq k+1$.

Case 1: $(k+1)$ divides a. Note $\gcd(a, k+1) = k+1$ in this case. The algorithm $\text{ExtGCD}(a, b)$ then runs Line 5 and returns $(k+1, 0, 1)$. Indeed, since $(k+1) = a \cdot 0 + (k+1) \cdot 1$, in this case the behavior of $\text{ExtGCD}(a, b)$ is correct.

Case 2: $a = (k+1)q + r$ and $0 < r \leq k$. From Theorem 1, we know $\gcd(a, k+1) = \gcd(k+1, r)$. The algorithm $\text{ExtGCD}(a, k+1)$ now proceeds to Line 7. In particular, it obtains (g, u, v) by calling $\text{ExtGCD}(k+1, r)$. Now note, $r \leq k$. Since $P(r)$ is true we get

- $g = \gcd(k+1, r)$ (I1)
- $g = u(k+1) + vr$ (I2)

The algorithm then *returns* (in Line 8) $(g, v, u - vq)$. We need to show this is correct behavior. That is, we

- Need to show $g = \gcd(a, k+1)$.
  Indeed, this follows from the fact that $\gcd(a, k+1) = \gcd(k+1, r)$ *and (I1).*
- Need to show $g = va + (u - vq) \cdot (k+1)$.
  Indeed, this is true since the RHS is $u(k+1) + v(a - (k+1)q)$. *Since* $a = (k+1)q + r$, *we get* $r = a - (k+1)q$, *and thus, we get* $u(k+1) + vr$ *which equals* g *from (I2).*

Therefore, we have proved $P(k+1)$. And therefore, by strong induction, the correctness of ExtGCD is established. □

Proof #2. We now give a proof of Theorem 2 using the "minimal counterexample idea." As mentioned earlier in the course, it is the same as the induction idea, said in a different language.

Suppose, for contradiction's sake, there exists positive numbers a, b such that for **no** two integers x, y, do we have $xa + yb = \gcd(a, b)$. Among *all* such *counterexample* pairs (a, b), let us pick a pair with the *smallest* sum $\min(a, b)$. That is, the smaller number in this pair is as small as possible.

Given this minimal counterexample (a, b), without loss of generality assume $a \geq b$ (otherwise swap names). Let us divide a by b to get $a = bq + r$ for some $0 \leq r < b$.

Suppose $r = 0$. That is, b divides a. Therefore, $\gcd(a, b) = b$ and since $0 \cdot a + 1 \cdot b = b$, we see that (a, b) cannot be a counterexample. Therefore, $r \neq 0$.

By Theorem 1 we know that $\gcd(a, b) = \gcd(b, r)$. Furthermore, $r = \min(b, r) < b = \min(a, b)$. Therefore, the two positive numbers (b, r) cannot be a counterexample to (Bezout's Identity) since (a, b) was the minimal counterexample. Which implies there exists integers x' and y' such that

$$x'b + y'r = \gcd(b, r) = g$$

However, $r = a - bq$. Substituting above, we get

$$x'b + y'(a - bq) = g \qquad \Rightarrow \qquad y'a + (x' - y'q)b = g$$

Thus, the integers $x = y'$ and $y = (x' - y'q)$ satisfy $xa + yb = g = \gcd(a, b)$. That is, (a, b) is not a counterexample. Contradiction. $\square$