Math 1365 (Intensive Mathematical Reasoning)

Lecture #12 of 35 $\sim$ October 4, 2023

GCDs and the Euclidean Algorithm

- GCDs
- Properties of GCDs
- The Euclidean Algorithm

This material represents §2.3.2-§2.3.3 from the course notes.

Reminder

Recall our result about division with remainder from last week:

Theorem (Division With Remainder)

If a and b are positive integers, then there exist unique integers q and r such that $a = qb + r$ with $0 \leq r < b$. Furthermore, $r = 0$ if and only if $b|a$.

GCDs, I

Our main goal today is to discuss the notion of the greatest common divisor of two integers:

Definition

If $d|a$ and $d|b$, then d is a common divisor of a and b.

GCDs, I

Our main goal today is to discuss the notion of the greatest common divisor of two integers:

Definition

If $d|a$ and $d|b$, then d is a common divisor of a and b.

Examples:

- 2 is a common divisor of 6 and 10, since $2|6$ and $2|10$. So are 1 and -2.
- The diviisors of 15 are $-15, -5, -3, -1, 1, 3, 5, 15$ and the divisors of 12 are $-12, -6, -4, -3, -2, -1, 1, 2, 3, 4, 6, 12$. The common divisors are $-3, -1, 1, 3$.

GCDs, II

If a and b are not both zero, then there are only a finite number of common divisors of a and b.

Definition

If a and b are integers, not both zero, then the greatest common divisor (GCD) of a and b is the greatest common divisor of a and b.

GCDs, II

If a and b are not both zero, then there are only a finite number of common divisors of a and b.

Definition

If a and b are integers, not both zero, then the greatest common divisor (GCD) of a and b is the greatest common divisor of a and b.

Okay, yes, when written out like this, it sounds circular, but that's just because the term defines itself! The GCD is just the largest of the common divisors.

GCDs, III

Example: Find the greatest common divisor of 30 and 42.

GCDs, III

Example: Find the greatest common divisor of 30 and 42.

- The positive divisors of 30 are 1, 2, 3, 5, 6, 10, 15, 30.
- The positive divisors of 42 are 1, 2, 3, 6, 7, 14, 21, 42.
- The common (positive) divisors are 1, 2, 3, and 6.
- The greatest of these is 6, so $\gcd(30, 42) = 6$.

Finding the GCD this way is pretty inefficient, because we have to write out all the divisors (which can be difficult with large numbers). We'll develop a better method later.

GCDs as Linear Combinations, I

Our first main result about greatest common divisors is that we can write them in terms of the original integers:

Theorem (GCD as Linear Combination)

If a and b are integers, not both zero, and $d = \gcd(a, b)$, then there exist integers x and y with $d = ax + by$. In fact, the gcd is the smallest positive such linear combination.

- This theorem says that the greatest common divisor of two integers is an integral linear combination of those integers.
- Example: We saw on the last slide that $\gcd(30, 42) = 6$. You can check that we can write $6 = 3 \cdot 30 - 2 \cdot 42$.

GCDs as Linear Combinations, II

Before we get going on the proof, let me point out a simplifying assumption we can make.

- We are given two integers a and b, not both zero.
- The details of the argument will depend a bit on which one is nonzero.
- We could write two separate arguments, one for each case.
- But the statement of our result is symmetric in a and b.
- So we can do the following trick: if $a = 0$, just swap a and b, so that now $a \neq 0$.
- There is a quick phrase for this sort of thing: "Without loss of generality, ...".

GCDs as Linear Combinations, III

Proof:

- Without loss of generality assume $a \neq 0$.
- Define the set $S = \{sa + tb : s, t \in \mathbb{Z}\} \cap \mathbb{Z}_+$ to be all positive integers of the form $sa + tb$ for some integers s, t.

GCDs as Linear Combinations, III

Proof:

- Without loss of generality assume $a \neq 0$.
- Define the set $S = \{sa + tb : s, t \in \mathbb{Z}\} \cap \mathbb{Z}_+$ to be all positive integers of the form $sa + tb$ for some integers s, t.
- Because either $-a$ or a is in S, we see S is nonempty.
- Therefore, by the well-ordering axiom of the integers, S contains a smallest element: let's call it l.
- We claim that l is actually the greatest common divisor of a and b.

GCDs as Linear Combinations, IV

Claim 1: The integer l (the smallest positive integer of the form $sa + tb$) is a common divisor of a and b. Let's say $l = sa + tb$.

- First let's show $l|a$. So divide a by l to write $a = ql + r$ for some $0 \leq r < l$. [Goal: Show $r = 0$.]

GCDs as Linear Combinations, IV

Claim 1: The integer l (the smallest positive integer of the form $sa + tb$) is a common divisor of a and b. Let's say $l = sa + tb$.

- First let's show $l|a$. So divide a by l to write $a = ql + r$ for some $0 \leq r < l$. [Goal: Show $r = 0$.]
- Rearrange to see that $r = a - ql = a - q(sa + tb) = (1 - qs)a + (-qt)b$.
- But look at this statement: it says r is some integer times a plus some other integer times b.
- If r were positive, then we'd have a contradiction to the assumption that l is the smallest positive integer of that form.
- So we must have $r = 0$! And so that means $l|a$.

GCDs as Linear Combinations, IV

Claim 1: The integer l (the smallest positive integer of the form $sa + tb$) is a common divisor of a and b. Let's say $l = sa + tb$.

- First let's show $l|a$. So divide a by l to write $a = ql + r$ for some $0 \leq r < l$. [Goal: Show $r = 0$.]
- Rearrange to see that $r = a - ql = a - q(sa + tb) = (1 - qs)a + (-qt)b$.
- But look at this statement: it says r is some integer times a plus some other integer times b.
- If r were positive, then we'd have a contradiction to the assumption that l is the smallest positive integer of that form.
- So we must have $r = 0$! And so that means $l|a$.

By the same exact argument, just with a, b swapped, we also see that $l|b$. So l is in fact a common divisor!

GCDs as Linear Combinations, V

Claim 2: The integer l (the smallest positive integer of the form $sa + tb$) is the greatest common divisor of a and b.

- We just saw that l is a common divisor, so now we only have to show it's the biggest.
- So suppose d is some other common divisor of a and b: then $d|a$ and $d|b$.
- But now since $l = sa + tb$ for some integers s and t, by our divisibility properties (or if you like, problem 4b of homework 4), that means $d|l$ too.

GCDs as Linear Combinations, V

Claim 2: The integer l (the smallest positive integer of the form $sa + tb$) is the greatest common divisor of a and b.

- We just saw that l is a common divisor, so now we only have to show it's the biggest.
- So suppose d is some other common divisor of a and b: then $d|a$ and $d|b$.
- But now since $l = sa + tb$ for some integers s and t, by our divisibility properties (or if you like, problem 4b of homework 4), that means $d|l$ too.
- If $d < 0$, then certainly $d < l$ since l is positive.
- Otherwise, if $d > 0$ then $d|l$ implies $d \leq l$, by another of our divisibility properties.
- That means every other common divisor of a, b is $\leq l$: in other words, l is the greatest.

GCDs as Linear Combinations, VI

So, now we know that for any integers a, b not both zero, there exist integers x and y such that $\gcd(a, b) = xa + yb$.

Corollary

Every common divisor of a and b divides their gcd. More explicitly, if $e|a$ and $e|b$, then $e|\gcd(a, b)$.

GCDs as Linear Combinations, VI

So, now we know that for any integers a, b not both zero, there exist integers x and y such that $\gcd(a, b) = xa + yb$.

Corollary

Every common divisor of a and b divides their gcd. More explicitly, if $e|a$ and $e|b$, then $e|\gcd(a, b)$.

Proof:

- By our result, there exist integers x and y such that $\gcd(a, b) = xa + yb$.
- But now if $e|a$ and $e|b$, then e also divides $xa + yb$ (divisibility properties), and $xa + yb$ is the gcd!

GCDs as Linear Combinations, VI

So, now we know that for any integers a, b not both zero, there exist integers x and y such that $\gcd(a, b) = xa + yb$.

Corollary

Every common divisor of a and b divides their gcd. More explicitly, if $e|a$ and $e|b$, then $e|\gcd(a, b)$.

Proof:

- By our result, there exist integers x and y such that $\gcd(a, b) = xa + yb$.
- But now if $e|a$ and $e|b$, then e also divides $xa + yb$ (divisibility properties), and $xa + yb$ is the gcd!

So, not only is the gcd the biggest of the common divisors, all other common divisors actually divide it!

GCDs as Linear Combinations, VII

Here are some more examples of these ideas:

1. We have $\gcd(5, 12) = 1$ and we can also write $5 \cdot 5 - 2 \cdot 12 = 1$. In fact, this relation proves the gcd must be 1, because any common divisor of 5 and 12 would also have to divide $5 \cdot 5 - 2 \cdot 12 = 1$.

GCDs as Linear Combinations, VII

Here are some more examples of these ideas:

1. We have $\gcd(5, 12) = 1$ and we can also write $5 \cdot 5 - 2 \cdot 12 = 1$. In fact, this relation proves the gcd must be 1, because any common divisor of 5 and 12 would also have to divide $5 \cdot 5 - 2 \cdot 12 = 1$.
2. We have $\gcd(8, 26) = 2$ since the positive divisors of 8 are 1,2,4,8 and the biggest that also divides 26 is 2. We can write $(-3) \cdot 8 + 1 \cdot 26 = 2$.

GCDs as Linear Combinations, VII

Here are some more examples of these ideas:

1. We have $\gcd(5, 12) = 1$ and we can also write $5 \cdot 5 - 2 \cdot 12 = 1$. In fact, this relation proves the gcd must be 1, because any common divisor of 5 and 12 would also have to divide $5 \cdot 5 - 2 \cdot 12 = 1$.
2. We have $\gcd(8, 26) = 2$ since the positive divisors of 8 are 1,2,4,8 and the biggest that also divides 26 is 2. We can write $(-3) \cdot 8 + 1 \cdot 26 = 2$.
3. You can check for yourself that $44 \cdot 102 - 13 \cdot 345 = 3$, so any common divisor of 102 and 345 must divide 3. But since 3 is a common divisor (note $102 = 34 \cdot 3$ and $345 = 105 \cdot 3$), 3 must be the gcd.

GCDs as Linear Combinations, VIII

The situation where two integers have gcd 1 comes up often, so we give it a name:

Definition

When $\gcd(a, b) = 1$, *we say* a *and* b *are relatively prime.*

Examples:

GCDs as Linear Combinations, VIII

The situation where two integers have gcd 1 comes up often, so we give it a name:

Definition

When $\gcd(a, b) = 1$*, we say* a *and* b *are relatively prime.*

Examples:

- 5 and 12 are relatively prime, since $\gcd(5, 12) = 1$.
- 2 and 13 are relatively prime, since $\gcd(2, 13) = 1$.
- 14 and 15 are relatively prime, since $\gcd(14, 15) = 1$.
- 30 and 66 are not relatively prime, since they have a common divisor $2 > 1$. (In fact their gcd is 6.)

If you are wondering why we call this "relatively prime", later we'll show that integers are relatively prime precisely when they have no prime factors in common.

Properties of GCDs, I

Let's establish a few more properties of GCDs:

Proposition

The following hold for integers m, a, b, d:

1. *If $m > 0$, then $\gcd(ma, mb) = m \cdot \gcd(a, b)$.*
2. *If $d > 0$ divides both a and b, then $\gcd(a/d, b/d) = \gcd(a, b)/d$.*
3. *There exist integers x and y with $xa + yb = 1$ if and only if $\gcd(a, b) = 1$. (i.e., if and only if a and b are relatively prime).*
4. *If a and b are both relatively prime to m, then so is ab.*
5. *For any integer x, $\gcd(a, b) = \gcd(a, b + xa)$.*
6. *If $a|bc$ and a and b are are relatively prime, then $a|c$.*

Properties of GCDs, II

1. If $m > 0$, then $\gcd(ma, mb) = m \cdot \gcd(a, b)$.

Proof:

Properties of GCDs, II

1. If $m > 0$, then $\gcd(ma, mb) = m \cdot \gcd(a, b)$.

Proof:

- From our results on gcds as linear combinations, $\gcd(ma, mb)$ is the smallest positive element of the set $S = \{mxa + myb : x, y \in \mathbb{Z}\}$, while $\gcd(a, b)$ is the smallest positive element of the set $T = \{xa + yb : x, y \in \mathbb{Z}\}$.

Properties of GCDs, II

1. If $m > 0$, then $\gcd(ma, mb) = m \cdot \gcd(a, b)$.

Proof:

- From our results on gcds as linear combinations, $\gcd(ma, mb)$ is the smallest positive element of the set $S = \{mxa + myb : x, y \in \mathbb{Z}\}$, while $\gcd(a, b)$ is the smallest positive element of the set $T = \{xa + yb : x, y \in \mathbb{Z}\}$.
- But because $mxa + myb = m(xa + yb)$, multiplying all of the elements of T by m yields the set S.
- In particular, if we take the smallest positive element of T and multiply it by m, this must give the smallest positive element of S.
- In other words, $\gcd(ma, mb) = m \cdot \gcd(a, b)$, as claimed.

Properties of GCDs, III

2. If $d > 0$ divides both a and b, then $\gcd(a/d, b/d) = \gcd(a, b)/d$.

Proof:

Properties of GCDs, III

2. If $d > 0$ divides both a and b, then $\gcd(a/d, b/d) = \gcd(a, b)/d$.

Proof:

- Remember that we just proved $\gcd(mp, mq) = m \cdot \gcd(p, q)$.
- Now apply this fact when $p = a/d$, $q = b/d$, and $m = d$.
- It yields $\gcd(a, b) = d \cdot \gcd(a/d, b/d)$.
- Now just divide both sides by d to get $\gcd(a, b)/d = \gcd(a/d, b/d)$, as desired.

Properties of GCDs, IV

3. There exist integers x and y with $xa + yb = 1$ if and only if $\gcd(a, b) = 1$ (i.e., if and only if a and b are relatively prime).

Proof:

Properties of GCDs, IV

3. There exist integers x and y with $xa + yb = 1$ if and only if $\gcd(a, b) = 1$ (i.e., if and only if a and b are relatively prime).

Proof:

- If $\gcd(a, b) = 1$ then our result on the GCD as a linear combination tells us there exist integers x and y with $xa + yb = 1$.
- For the other direction, any common divisor (in particular, the gcd) of a and b must divide $xa + yb = 1$.
- But that means the gcd must divide 1, which since the gcd is positive, means the gcd must equal 1.

Properties of GCDs, V

4. If a and b are both relatively prime to m, then so is ab.

Proof:

Properties of GCDs, V

4. If a and b are both relatively prime to m, then so is ab.

Proof:

- By the linear combination property of the gcd, there exist x_1, y_1, x_2, y_2 with $ax_1 + my_1 = 1$ and $bx_2 + my_2 = 1$.
- Multiplying these two equations together and rearranging the results yields $ab(x_1x_2) + m(y_1bx_2 + y_2ax_1 + my_1y_2) = 1$.
- This last fact implies that ab is relatively prime to m, because it is a relation of the form $\triangle \cdot ab + \square \cdot m = 1$, and as we just showed on the last slide, this particular relation implies $\gcd(ab, m) = 1$.

Properties of GCDs, VI

5. For any integer x, $\gcd(a, b) = \gcd(a, b + xa)$.

Proof:

Properties of GCDs, VI

5. For any integer x, $\gcd(a, b) = \gcd(a, b + xa)$.

Proof:

- We show a, b and $a, b + xa$ have the same common divisors: that [$d|a$ and $d|b$] if and only if [$d|a$ and $d|(b + xa)$].
- First suppose $d|a$ and $d|b$.
- Then $d|a$ and $d|(b + ax)$, so d is also a common divisor of a and $b + ax$.

Properties of GCDs, VI

5. For any integer x, $\gcd(a, b) = \gcd(a, b + xa)$.

Proof:

- We show a, b and $a, b + xa$ have the same common divisors: that [$d|a$ and $d|b$] if and only if [$d|a$ and $d|(b + xa)$].
- First suppose $d|a$ and $d|b$.
- Then $d|a$ and $d|(b + ax)$, so d is also a common divisor of a and $b + ax$.
- Conversely, now suppose $e|a$ and $e|(b + ax)$.
- Then $e|a$ and $e|[(b + ax) - x \cdot a]$, which is to say, $e|a$ and $e|b$, so e is a common divisor of a and b.
- This shows both implications, so we are done. Since a, b and $a, b + xa$ have the same common divisors, their greatest common divisors are also the same.

Properties of GCDs, VIII: The Last Jedi

6. If $a|bc$ and a and b are are relatively prime, then $a|c$.

Proof 1:

Properties of GCDs, VIII: The Last Jedi

6. If $a|bc$ and a and b are are relatively prime, then $a|c$.

Proof 1:

- From property (1) at the beginning, we have $\gcd(ac, bc) = c \cdot \gcd(a, b) = c$.
- Now because $a|bc$ and $a|ac$, we see that a is a common divisor of ac and bc.
- Since every common divisor divides the gcd, that means a divides $\gcd(ac, bc) = c$. So $a|c$, as claimed.

This proof is nice, but let me give you another one just for fun.

Properties of GCDs, IX: The Reprovening

6. If $a|bc$ and a and b are are relatively prime, then $a|c$.

Proof 2:

Properties of GCDs, IX: The Reprovening

6. If $a|bc$ and a and b are are relatively prime, then $a|c$.

Proof 2:

- Since a and b are relatively prime, by (3) from earlier, there exist integers x and y with $ax + by = 1$.
- Multiplying both sides by c yields $acx + bcy = c$.
- Now observe that a divides both acx and bcy, so it divides their sum c.

These proofs look very different, but they actually use the same idea in the middle. Can you see what it is?

LCMs, I

Before we talk about how to calculate gcds, let's take a few minutes to mention a concept that's very similar to the gcd: the least common multiple.

Definition

If $a|l$ and $b|l$, we say l is a common multiple of a and b. Among all (nonnegative) common multiples of a and b, the smallest such l is the least common multiple of a and b, denoted $\text{lcm}(a, b)$.

LCMs, I

Before we talk about how to calculate gcds, let's take a few minutes to mention a concept that's very similar to the gcd: the least common multiple.

Definition

If $a|l$ and $b|l$, we say l is a common multiple of a and b. Among all (nonnegative) common multiples of a and b, the smallest such l is the least common multiple of a and b, denoted $\text{lcm}(a, b)$.

- Example: The least common multiple of 30 and 42 is 210, as follows by noting that $210 = 7 \cdot 30 = 5 \cdot 42$ and that none of $1 \cdot 42$, $2 \cdot 42$, $3 \cdot 42$, and $4 \cdot 42$ is divisible by 30.

Least common multiples often show up in elementary school for finding the "least common denominator" when adding fractions.

LCMs, II

The lcm has fewer nice properties than the gcd, but it turns out that we can obtain either one from the other:

Proposition

For any positive integers m, a, b, the following hold:

1. *We have* $\operatorname{lcm}(ma, mb) = m \cdot \operatorname{lcm}(a, b)$.
2. *We have* $\gcd(a, b) \cdot \operatorname{lcm}(a, b) = ab$.

LCMs, II

The lcm has fewer nice properties than the gcd, but it turns out that we can obtain either one from the other:

Proposition

For any positive integers m, a, b, the following hold:

1. *We have* $\operatorname{lcm}(ma, mb) = m \cdot \operatorname{lcm}(a, b)$.
2. *We have* $\gcd(a, b) \cdot \operatorname{lcm}(a, b) = ab$.

- So for example, because we calculated earlier that $\gcd(30, 42) = 6$, item (2) says that $\operatorname{lcm}(30, 42) = 30 \cdot 42/6 = 210$, exactly as calculated on the previous slide.

LCMs, III

1. We have $\mathrm{lcm}(ma, mb) = m \cdot \mathrm{lcm}(a, b)$.

Proof:

LCMs, III

1. We have $\mathrm{lcm}(ma, mb) = m \cdot \mathrm{lcm}(a, b)$.

Proof:

- Since ma divides $\mathrm{lcm}(ma, mb)$, the lcm is a multiple of ma hence of m, so $\mathrm{lcm}(ma, mb) = mk$ for some integer k.
- Then $ma|mk$ and $mb|mk$, so a and b both divide k. Thus $k \geq l$, where $l = \mathrm{lcm}(a, b)$.

LCMs, III

1. We have $\mathrm{lcm}(ma, mb) = m \cdot \mathrm{lcm}(a, b)$.

Proof:

- Since ma divides $\mathrm{lcm}(ma, mb)$, the lcm is a multiple of ma hence of m, so $\mathrm{lcm}(ma, mb) = mk$ for some integer k.
- Then $ma|mk$ and $mb|mk$, so a and b both divide k. Thus $k \geq l$, where $l = \mathrm{lcm}(a, b)$.
- On the other hand, since $a|l$ and $b|l$ we see $ma|ml$ and $mb|ml$, so ml is a common multiple, hence $ml \geq mk$ and so $l \geq k$.
- But $k \geq l$ and $l \geq k$ imply $l = k$, and this means $\mathrm{lcm}(ma, mb) = m \cdot \mathrm{lcm}(a, b)$ as claimed.

LCMs, IV

2. We have $\gcd(a, b) \cdot \operatorname{lcm}(a, b) = ab$.

Proof:

LCMs, IV

2. We have $\gcd(a, b) \cdot \operatorname{lcm}(a, b) = ab$.

Proof:

- First we show the result when a, b are relatively prime, in which case we need to show $\operatorname{lcm}(a, b) = ab$. Since ab is clearly a common multiple of a and b, we just want to show it's the smallest.

LCMs, IV

2. We have $\gcd(a, b) \cdot \operatorname{lcm}(a, b) = ab$.

Proof:

- First we show the result when a, b are relatively prime, in which case we need to show $\operatorname{lcm}(a, b) = ab$. Since ab is clearly a common multiple of a and b, we just want to show it's the smallest.
- So suppose l is a common multiple. Then since $a|l$ we can write $l = ak$ for some integer k.
- But because $b|ak$ and $\gcd(a, b) = 1$, by the relatively-prime divisibility property from earlier we deduce that $b|k$, meaning that $k \geq b$ and thus $l \geq ab$ as desired.

LCMs, IV

2. We have $\gcd(a, b) \cdot \operatorname{lcm}(a, b) = ab$.

Proof:

- First we show the result when a, b are relatively prime, in which case we need to show $\operatorname{lcm}(a, b) = ab$. Since ab is clearly a common multiple of a and b, we just want to show it's the smallest.
- So suppose l is a common multiple. Then since $a|l$ we can write $l = ak$ for some integer k.
- But because $b|ak$ and $\gcd(a, b) = 1$, by the relatively-prime divisibility property from earlier we deduce that $b|k$, meaning that $k \geq b$ and thus $l \geq ab$ as desired.
- In the general case, let $d = \gcd(a, b)$. Then $\gcd(a/d, b/d) = \gcd(a, b)/d = 1$, so by the above we have $\operatorname{lcm}(a/d, b/d) = (a/d) \cdot (b/d) = ab/d^2$. Then by (1), $\gcd(a, b) \cdot \operatorname{lcm}(a, b) = d \cdot d \operatorname{lcm}(a/d, b/d) = ab$, as claimed.

The Euclidean Algorithm, I

Now, at last, we can actually talk about how to calculate GCDs.

Theorem (Euclidean Algorithm)

Given integers $0 < b < a$, repeatedly apply the division algorithm as follows, until a remainder of zero is obtained:

$$\begin{aligned} a &= q_1 b + r_1 \\ b &= q_2 r_1 + r_2 \\ r_1 &= q_3 r_2 + r_3 \\ &\vdots \\ r_{k-1} &= q_{k+1} r_k + r_{k+1} \\ r_k &= q_{k+2} r_{k+1}. \end{aligned}$$

Then $\gcd(a, b)$ is equal to the last nonzero remainder, r_{k+1}. Furthermore, by successively solving for the remainders and plugging in the previous equations, r_{k+1} can be explicitly written as a linear combination of a and b.

The Euclidean Algorithm, II

Example: Find $\gcd(30, 42)$ using the Euclidean algorithm, and write the gcd explicitly as a linear combination of 30 and 42.

The Euclidean Algorithm, II

Example: Find $\gcd(30, 42)$ using the Euclidean algorithm, and write the gcd explicitly as a linear combination of 30 and 42.

- First, we use the Euclidean algorithm:

$$\begin{aligned} 42 &= 1 \cdot 30 + 12 \\ 30 &= 2 \cdot 12 + 6 \\ 12 &= 2 \cdot 6 \end{aligned}$$

  so the gcd is the last nonzero remainder $\boxed{6}$.

- For the linear combination, we solve for the remainders:

$$\begin{aligned} 12 &= 42 - 1 \cdot 30 &&= 1 \cdot 42 - 1 \cdot 30 \\ 6 &= 30 - 2 \cdot 12 &&= 30 - 2(42 - 1 \cdot 30) &&= -2 \cdot 42 + 3 \cdot 30 \end{aligned}$$

  so we obtain $\boxed{6 = -2 \cdot 42 + 3 \cdot 30}$.

The Euclidean Algorithm, III

Example: Find $\gcd(133, 98)$ using the Euclidean algorithm, and write the gcd explicitly as a linear combination of 133 and 98.

The Euclidean Algorithm, III

Example: Find $\gcd(133, 98)$ using the Euclidean algorithm, and write the gcd explicitly as a linear combination of 133 and 98.

- First, we use the Euclidean algorithm:

$$\begin{aligned} 133 &= 1 \cdot 98 + 35 \\ 98 &= 2 \cdot 35 + 28 \\ 35 &= 1 \cdot 28 + 7 \\ 28 &= 4 \cdot 7 \end{aligned}$$

  and so the gcd is $\boxed{7}$.

- For the linear combination, we solve for the remainders:

$$\begin{aligned} 35 &= 133 - 1 \cdot 98 &&= 1 \cdot 133 - 1 \cdot 98 \\ 28 &= 98 - 2 \cdot 35 &&= -2 \cdot 133 + 3 \cdot 98 \\ 7 &= 35 - 1 \cdot 28 &&= 3 \cdot 133 - 4 \cdot 98 \end{aligned}$$

  so we obtain $\boxed{7 = 3 \cdot 133 - 4 \cdot 98}$.

The Euclidean Algorithm, IV

Let's now show that the Euclidean algorithm works. There are a few pieces to this:

- First, we need to see that the algorithm will always terminate (i.e., it won't continue going forever without returning a result).
- That's not too hard to see, because each remainder is strictly less than the previous one: $b > r_1 > r_2 > \cdots \geq 0$. Then the well-ordering axiom dictates that we cannot have an infinite decreasing sequence of nonnegative integers.
- So we must eventually get a remainder of zero, and then the algorithm terminates.

The Euclidean Algorithm, V

Second: We need to show that if $d|a$ and $d|b$, then $d|r_{k+1}$ (the last nonzero remainder).

- We will show more: that if $d|a$ and $d|b$ then in fact $d|r_n$ for all n. We use induction on n.
- A cheap way to avoid having to do too much work is to denote $r_0 = b$ and $r_{-1} = a$, and then start with these two remainders.
- So: we take base cases $k = -1$ and $k = 0$: then $d|r_{-1} = a$ and $d|r_0 = b$.
- For the inductive step suppose $d|r_k$ and $d|r_{k-1}$. Then $r_{k+1} = r_{k-1} - q_k r_k$. Since both terms r_{k-1} and $q_k r_k$ are divisible by d, so is their difference r_{k+1}.

The Euclidean Algorithm, VI

Third: We show that $r_{k+1}|a$ and $r_{k+1}|b$. Combined with the previous slide this will show r_{k+1} is the gcd, since it's a common divisor divisible by all the other common divisors.

- For this we induct "downwards" by showing $r_{k+1}|r_n$ for all n.

The Euclidean Algorithm, VI

Third: We show that $r_{k+1}|a$ and $r_{k+1}|b$. Combined with the previous slide this will show r_{k+1} is the gcd, since it's a common divisor divisible by all the other common divisors.

- For this we induct "downwards" by showing $r_{k+1}|r_n$ for all n.
- For base cases we observe $r_{k+1}|r_{k+1}$ and $r_{k+1}|r_k$ because $r_k = q_{k+1}r_{k+1}$.
- For the inductive step we observe $r_{n-1} = q_{n+1}r_n + r_{n+1}$, and by hypothesis the last nonzero remainder divides both r_n and r_{n+1}, so it also divides r_{n-1}.
- Moving all the way downward we see that r_{k+1} divides $r_0 = b$ and then $r_{-1} = a$, as desired.

The Euclidean Algorithm, VII

Finally, we need to see that the last nonzero remainder can be written in terms of the original integers.

- It may not surprise you, but this follows from another induction argument!
- Explicitly, for base cases we take $r_{-1} = a = 1 \cdot a + 0 \cdot b$ and $r_0 = b = 0 \cdot a + 1 \cdot b$.
- For the inductive step, if we can write r_{n-1} and r_n in terms of a, b, then since $r_{n+1} = r_{n-1} - q_{n+1} r_n$, plugging in those expressions will yield r_{n+1} in terms of a, b as well.

And that establishes the correctness of the Euclidean algorithm! (Yay.)

Summary

We discussed greatest common divisors and some of their properties.

We discussed the Euclidean algorithm and how to use it to calculate greatest common divisors.

Next lecture: Primes and unique prime factorization.