1.2: GCDs and their properties

May 8, 2012

Outline

Recall the Division Algorithm

- Given integers a, b, with $a > 0$, there exist unique integers q and r such that $b = qa + r$, $0 \leq r < a$.
- We will prove this theorem, and then use it to prove a fundamental fact about GCDs in the next section.
- We first prove that there is such an r and q, then prove r and q are unique.

Proof: existence

- Consider set of all $b \pm ka$.
- Well-ordering $\implies$ there is a smallest element.
- $r =$ this smallest element.
- $r = b - qa$

Proof: uniqueness

Suppose q_1, r_1 is another pair.

- $r < r_1$ by choice of r.
- $0 < r - r_1 = a(q - q_1) < a$ (since $r < a$)
- Thus $a | r - r_1$. So a divides a number smaller than it in absolute value.
- This contradicts a fact about $|$ from lecture 1.
- $r = r_1$. Hence $q = q_1$.

Outline

Definition

A *common divisor* of two numbers b, c is an integer a such that $a|b$ and $a|c$.

- There are a finite number of divisors of any non-zero integer.
- Because if $a|c$ then $-c \leq a \leq c$.
- Thus there are a finite number of common divisors.
- Unless $b = c = 0$.

Definition

A *common divisor* of two numbers b, c is an integer a such that $a|b$ and $a|c$.

- There are a finite number of divisors of any non-zero integer.
- Because if $a|c$ then $-c \leq a \leq c$.
- Thus there are a finite number of common divisors.
- Unless $b = c = 0$.

Definition

A *common divisor* of two numbers b, c is an integer a such that $a|b$ and $a|c$.

- There are a finite number of divisors of any non-zero integer.
- Because if $a|c$ then $-c \leq a \leq c$.
- Thus there are a finite number of common divisors.
- Unless $b = c = 0$.

Definition

A *common divisor* of two numbers b, c is an integer a such that $a|b$ and $a|c$.

- There are a finite number of divisors of any non-zero integer.
- Because if $a|c$ then $-c \leq a \leq c$.
- Thus there are a finite number of common divisors.
- Unless $b = c = 0$.

Examples

- $b = 14, c = 21$: $-7, -1, 1, 7$
- $b = 36, c = 54$: $\pm 18, \pm 9, \pm 6, \pm 3, \pm 2, \pm 1$
- $b = 1, c = 14$: ± 1
- $b = 0, c = 14$: $\pm 14, \pm 7, \pm 2, \pm 1$
- $b = 14, c = 14$: $\pm 14, \pm 7, \pm 2, \pm 1$

linear combinations

Recall from lecture 1: If $a|b$ and $a|c$ then $a|(x_0b + y_0c)$.

- Thus a common divisor also divides $\mathbb{Z}-$linear combinations.

Greatest common divisors

Since there are a finite number of common divisors, there is a greatest one.

- Note well-ordering again.
- Of course well-ordering = induction.

Examples

- $(14, 21) = 7$
- $(36, 54) = 18$
- $(1, 14) = 1$
- $(0, 14) = 14$
- $(14, 14) = 14$

GCD is always positive!

Outline

The Identity

If g is the common divisor of b and c, then there exist x_0, y_0 such that

$$g = (b, c) = bx_0 + cy_0.$$

- First known statement is Méziriac in the 1600s
- Most often called Bézout identity, but he proved it for polynomials.
- The gcd is expressible as a $\mathbb{Z}$-linear combination of the two integers.
- Recall that any common divisor divides $\mathbb{Z}$-linear combinations.x1
- So this is a sort of converse.

Proof Outline

1. Choose the smallest (positive) $\mathbb{Z}$-linear combination, l.
2. Prove that l is a common divisor using the division algorithm and proof by contradiction (using the choice of l).
3. Note that a common divisor divides any $\mathbb{Z}$-linear combination, thus $g|l$. Conclude the theorem.

Step 2

(Step 1 and 3 being easy).

- Without loss of generality, only prove $l|b$.
- Assume l does not divide b.
- Division algorithm gives $r > 0$ such that $r = b - lq$.
- $b - lq = b(1 - qx_0) + c(-qy_0)$ so r is in the set l is chosen from.
- Thus $r > l$. This contradicts the choice of r from the division algorithm.

Consequence

We could have defined GCD this way:

Theorem

The greatest common divisor of b and c is the least positive $\mathbb{Z}$-linear combination of b and c.

Or this way:

Theorem

The greatest common divisor of b and c is the positive common divisor that is divisible by every other common divisor.

Outline

Common factors

Theorem

For any positive integer m,

$$(ma, mb) = m(a, b)$$

Proof.

(ma, mb) is the least positive value of $max + mby$, which is the same as the least positive value of $ax + by$ times m. □

Common factors

Theorem

If $d|a$ and $d|b$ and $d > 0$ then

$$(\frac{a}{d}, \frac{b}{d}) = \frac{1}{d}(a, b)$$

This is just a restatement of the previous statement.

What do these common factor statements mean?

What we are really saying is, by definition:

$$g = (a, b)$$

$$\left(\frac{a}{g}, \frac{b}{g}\right) = 1$$

i.e. dividing doesn't do something non-atomic.

Relatively prime pairs

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

Proof.

By the Méziriac-Bézout identity

$$1 = ax_0 + my_0 = bx_1 + my_1$$

$$1 = 1 \cdot 1 = abx_0x_1 + m(Stuff)$$

i.e. by the identity again $ab, m) = 1$. □

Thus, multiplying doesn't create new factors.

relatively prime

Note: We used the term relatively prime. Above. It's defined how you think.

One must fall!

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

Outline

general addition

In general addition is screwy:

$$(12, 2) = 2$$

$$(12, 3) = 3$$

$$(12, 4) = 4$$

$$(12, 5) = 1$$

Adding multiples

But ...

Theorem

$$d = (a, b) = (a, b + ax)$$

This isn't as satisfying as the results on division/multiplication, but next lecture we will see it is very powerful.

Proof Outline

Let,

$$d = (a, b)$$

$$g = (a, b + ax)$$

1. Show that $d | b + ax$.
2. Show $g | d$.
3. Since $d | b + ax$, by lecture 1 $d | g$.
4. Conclude $d = \pm g$.
5. Since $d, g > 0$ $d = g$.

Show $d|b + ax$

Since $d|a$ and $d|b$ by definition, we have by the linear combination property from lecture 1 that $d|b + ax$.

Show $g|d$.

By the Méziriac-Bézout identity there are x_0 and y_0:

$$d = ax_0 + by_0$$

$$d = a(x_0 - xy_0) + (b + ax)y_0$$

Since d is a linear combination of a and $(b + ax)$ by the definition of g and the linear combination property from lecture 1, we have $g|d$.