Greatest common divisor, part 2

MTH 350 -- Module 3B

Given any two integers a, b (not both zero), $\gcd(a, b)$ is always positive.

True

False

To 0

Given any two integers a, b (not both zero), $\gcd(a, b)$ can be written as an integer linear combination of a and b.

True

False

Given any two integers a, b (not both zero), $\gcd(a, b)$ divides every possible integer linear combination of a and b.

True

False

To 0

Prove that last statement in your groups. A simpler version works just as well:

If $d|a$ and $d|b$, then $d|(ax+by)$ for any integers x,y.

Implications of Bezout’s Identity

Theorem 3.10

Let a,b be integers not both zero. Then not only is gcd(a,b) a linear combination of a and b, it is the SMALLEST POSITIVE linear possible of a and b.

→ gcd(a,b) is a linear combination of a,b: That’s Bezout’s Identity
→ gcd(a,b) is always positive: From your polling activity
→ gcd(a,b) is the smallest positive LC possible: From your proof

Corollary 3.11

Let a,b be integers not both zero. Then gcd(a,b) = 1 if and only if there exist integers x,y such that ax + by =1.

(⇒) This is Bezout's Identity.

(⇐) **Not** because of Bezout's Identity! Use Theorem 3.10 instead.

Two integers a,b are **relatively prime** if gcd(a,b) = 1.

What's this for?

Integers that are relatively prime play important roles in high-level applications of arithmetic and algebra, like cryptography:

Key Generation

Select p, q	p and q both prime
Calculate $n = p \times q$	
Calculate $\phi(n) = (p-1)(q-1)$	
Select integer e	$\gcd(\phi(n), e) = 1;\ 1 < e < \phi(n)$
Calculate d	$d \equiv e^{-1} \bmod \phi(n)$
Public key	$KU = \{e, n\}$
Private key	$KR = \{d, n\}$

Encryption

Plaintext	$M < n$
Ciphertext	$C = M^e \pmod{n}$

Decryption

Ciphertext	C
Plaintext	$M = C^d \pmod{n}$

More about gcd’s and relative primality

Theorem 3.14. *Let a and b be integers, not both zero, and let $d = \gcd(a, b)$. Then $\frac{a}{d}$ and $\frac{b}{d}$ are relatively prime integers.*

Proof. Since $d = \gcd(a, b)$, it follows that both $\frac{a}{d}$ and $\frac{b}{d}$ are integers. Furthermore, there exist integers x and y such that

$$d = ax + by.$$

From this it follows that

$$1 = \frac{a}{d} \cdot x + \frac{b}{d} \cdot y,$$

which implies that $\gcd\left(\frac{a}{d}, \frac{b}{d}\right) = 1$, as desired. ∎

Theorem 3.15. *Let a, b, and d be integers, with a and b not both zero. Then $d = \gcd(a, b)$ if and only if all of the following conditions hold:*

(i) *$d \mid a$ and $d \mid b$.*

(ii) *If k is an integer such that $k \mid a$ and $k \mid b$, then $k \mid d$ also.*

(iii) *d is positive.*

Activity 3.16. Let a, b, and d be integers, with a and b not both zero.

(a) Suppose $d = \gcd(a, b)$. Explain why conditions (i) and (iii) from Theorem 3.15 are automatically satisfied. Then use Bezout's Identity to prove condition (ii).

(b) Now suppose d is an integer that satisfies all three of the conditions from Theorem 3.15. Explain why there cannot exist an integer $k > d$ such that $k \mid a$ and $k \mid b$.

Activity 3.18. Decide whether each of the following statements is true or false. For those that are true, explain why. For those that are false, give a counterexample and then change **one word or symbol** in the statement to make it true. For each statement, assume that a, b, and d are positive integers.

(a) If $ax + by = 1$ for some integers x and y, then $\gcd(a, b) = 1$.

(b) If $ax + by \neq 1$ for some integers x and y, then $\gcd(a, b) \neq 1$.

(c) If $ax + by = d$ for some integers x and y, then $\gcd(a, b) = d$.

Exercises

(1) Let a be an integer. After looking at several examples, make a general conjecture about the value of $\gcd(a-1, a+1)$. Then prove your conjecture.

(2) Fill in the blank, and prove your answer: For every integer a,

$$\gcd(a, a+1) = \underline{\qquad}.$$

Feedback:

http://gvsu.edu/s/1zN