Number Theory: 
GCD's & linear combinations

Arithmetic Assumptions
assume usual rules for +, ·, -:
a \cdot (b+c) = ab + ac, \ a \cdot b = ba, 
(ab)c = a \cdot (bc), \ a - a = 0,
a + 0 = a, \ a+1 > a, ....

The Division Theorem
For \( b > 0 \) and any \( a \), have 
\[ q = \text{quotient}(a,b) \]
\[ r = \text{remainder}(a,b) \]
\[ \exists \text{unique numbers } q, r \text{ such that } a = qb + r \text{ and } 0 \leq r < b. \]
Take this for granted too!

Divisibility
\[ c \text{ divides } a \ (c|a) \text{ iff } a = k \cdot c \text{ for some } k \]
5|15 because 15 = 3 \cdot 5
n|0 because 0 = 0 \cdot n
Simple Divisibility Facts

• \( c \mid a \) implies \( c \mid (sa) \)

\[ a = k'c \text{ implies } (sa) = (sk')c \]

\[ k \]

Simple Divisibility Facts

• \( c \mid a \) implies \( c \mid (sa) \)

• if \( c \mid a \) and \( c \mid b \) then

\( c \mid (a+b) \)

\[ \text{if } a = k_1c, b = k_2c \text{ then } a + b = (k_1 + k_2)c \]

Common Divisors

Common divisors of \( a \) & \( b \) divide integer linear combinations of \( a \) & \( b \).
gcd(a,b) ::= the greatest common divisor of a and b

gcd(10,12) = 2
gcd(13,12) = 1
gcd(17,17) = 17
gcd(0, n) = n \text{ for } n > 0

Lemma: p prime implies gcd(p,a) = 1 or p

Proof: The only divisors of p are \pm 1 \text{ and } \pm p.