Mathematics for Computer Science
MIT 6.042J/18.062J

Number Theory: GCD's & linear combinations

Arithmetic Assumptions

assume usual rules for +, $\cdot$, - :

$a(b+c) = ab + ac$, $ab = ba$,

$(ab)c = a(bc)$, $a - a = 0$,

$a + 0 = a$, $a+1 > a$, ...

The Division Theorem

For $b > 0$ and any a, have

q = quotient(a,b)

r = remainder(a,b)

$\exists$ unique numbers q, r such that

$a = qb + r$ and $0 \leq r < b$.

Take this for granted too!

Divisibility

c divides a ($c|a$) iff

$a = k \cdot c$ for some k

$5|15$ because $15 = 3 \cdot 5$

$n|0$ because $0 = 0 \cdot n$

Simple Divisibility Facts

- $c|a$ implies $c|(sa)$

[$a=k'c$ implies

$$(sa)=\underbrace{(sk')}_{k}c]$$

Simple Divisibility Facts

- $c|a$ implies $c|(sa)$
- if $c|a$ and $c|b$ then

$$c|(a+b)$$

[if $a=k_1c$, $b=k_2c$ then

$$a+b=(k_1+k_2)c\ ]$$

Simple Divisibility Facts

- if $\overbrace{c|a \text{ and } c|b}^{c \text{ a common divisor of } a,b}$ then

$$c|\underbrace{(sa+tb)}_{\text{integer linear combination of } a \text{ and } b}$$

Common Divisors

Common divisors of a & b divide integer linear combinations of a & b.

GCD

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 for $n>0$

GCD

gcd(a,b) ::= the greatest common divisor of a and b

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

proof: The only divisors of p are ± 1 & $\pm p$.