Mathematics for Computer Science

MIT 6.042J/18.062J

Intro to Number Theory: Divisibility, GCD's

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

c a common divisor of a,b

- if $\overbrace{c|a \text{ and } c|b}$ 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

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

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

GCD is a linear combination

Theorem:

gcd(a,b) is an integer linear combination of a and b.

gcd(a,b) = sa+tb

Proof: Show how to find coefficients s,t.

Method: apply Euclidean algorithm, finding coefficients as you go.

Finding s and t

Example: a = 899, b=493

899 = 1·493 + 406	so 406 = 1·899 + -1·493
493 = 1·406 + 87	so 87 = 493 – 1·406
	= -1·899 + 2·493
406 = 4·87 + 58	so 58 = 406 - 4·87
	= 5·899 + -9·493
87 = 1·58 + 29	so 29 = 87 – 1·58
	= -6·899 + 11·493
58 = 2·29 + 0	done, gcd = 29

Finding s and t

Example: a = 899, b=493

899 = 1·493 + 406 so 406 = 1·899 + -1·493

493 = 1·406 + 87 so 87 = 493 – 1·406
= -1·899 + 2·493

406 = 4·87 + 58 so 58 = 406 - 4·87
= 5·899 + -9·493

87 = 1·58 + 29 so 29 = 87 – 1·58
= -6·899 + 11·493

58 = 2·29 + 0 done, gcd = 29

the Pulverizer s = -6, t = 11

Finding s > 0 and t

gcd(899,493) = -6·899 + 11·493

get positive coeff. for 899?:

(-6+493k)·899 + (11-899k)·493

= -6·899 + 11·493

so use k=1: 487·899 + -888·493

= gcd(899,493)

Prime Divisibility

Lemma: p prime and $p|(a \cdot b)$ implies $p|a$ or $p|b$

pf: in Class Problem 3.

Prime Divisibility

Cor :If p is prime, and

$p|a_1 \cdot a_2 \cdot \cdots \cdot a_m$

then $p|a_i$ for some i.

pf: By induction on m.

Fundamental Thm. of Arithmetic

Every integer > 1 factors uniquely into a weakly increasing sequence of primes

Unique Prime Factorization

Every integer n > 1 has a unique factorization into primes: $p_0 \cdot p_1 \cdot \cdots \cdot p_k = n$

with $p_0 \leq p_1 \leq \cdots \leq p_k$

Unique Prime Factorization

Fundamental Theorem of Arithmetic

Example:

61394323221 =

$3 \cdot 3 \cdot 3 \cdot 7 \cdot 11 \cdot 11 \cdot 37 \cdot 37 \cdot 37 \cdot 53$

Unique Prime Factorization

pf: suppose not. choose smallest $n > 1$:

$$n = p_1 \cdot p_2 \cdots p_k = q_1 \cdot q_2 \cdots q_m$$

$$p_1 \leq p_2 \leq \cdots \leq p_k$$

$$q_1 \leq q_2 \leq \cdots \leq q_m$$

can assume $q_1 < p_1$

so $q_1 \neq$ any p_i

Unique Prime Factorization

Pf: but $q_1 | n$ & $n = p_1 \cdot p_2 \cdots p_k$

so $q_1 | p_i$ for some i by Cor,

contradicting that p_i is prime QED

Team Problems

Problems 1—3

6.042J / 18.062J Mathematics for Computer Science
Spring 2010