Mathematics for Computer Science

MIT 6.042J/18.062J

Intro to Number Theory: Divisibility, GCD's

Arithmetic Assumptions

Algebraic rules for +, -, ×:

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

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

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

We take these for granted!

Divisibility

a "divides" b (a|b):

$b = ak$ for some k

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

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

Simple Divisibility Facts

$a|b$ implies $a|bc$

$a|b$ and $b|c$ implies $a|c$

$a|b$ iff $ac|bc$

for $c \neq 0$

Common Divisors, GCD

c is a common divisor of a and b means $c|a$ and $c|b$.

$\gcd(a,b)$ ::= the *greatest* common divisor of a and b.

GCD with a prime

If p is prime, and p does not divide a, then

$\gcd(p,a) = 1$.

Pf: The only divisors of p are 1 & p.

Divisibility of a Sum

A common divisor of two terms divides their sum.

pf: say $c|x$ and $c|y$, so $x=k'c$, $y=k''c$. Then

$$x+y = k'c+k''c = c(\underbrace{k'+k''}_{k}).$$

Divisibility of Linear Comb.

A common divisor of a & b divides any integer linear combination of a & b.

integer lin. comb.: $sa + tb$

proof: divisor of a & b divides both sa and tb.

The Division Theorem

For $b > 0$ and any a, there are *unique* numbers

q ::= quotient(a,b),

r ::= remainder(a,b), such that

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

Take this for granted too!

Corollary

The remainder of a divided by b is an integer linear combination of a & b:

$$a = qb + r, \quad \text{so}$$
$$r = (-q)\cdot b + 1\cdot a$$

GCD is a linear combination

Theorem: gcd(a,b) is the smallest positive linear combination of a and b.

spc(a,b)

1st show: gcd(a,b) ≤ spc(a,b)

proof: Common divisor of a, b divides lin. comb. of a & b, so

$$gcd(a,b) \mid spc(a,b).$$

In particular,

$$gcd(a,b) \leq spc(a,b).$$

2nd: spc(a,b) $\leq$ gcd(*a*,*b*)

Enough to show that spc(a,b) is a common divisor of *just a*.

Lemma: spc(a,b)|a

Pf: Remainder of a divided by spc(a,b), is a linear comb. of a & b. Since remainder < divisor, and divisor is smallest positive, remainder must be 0. That is, spc(a,b) divides a.

Prime Divisibility

Lemma: p prime and p|a·b implies p|a or p|b.

pf: say ¬(p|a). so gcd(p,a)=1.

so, $sa + tp = 1$

$(sa)b + (tp)b = b$

$p|$ $p|$ so $p|$

QED

Prime Divisibility

Cor: If p is prime, and $p|a_1 \cdot a_2 \cdots a_m$ then $p|a_i$ for some i.

pf: By induction on m.

Finding s and t

Given a,b, how to find s,t so that sa+tb=gcd(a,b)?

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

Finding s and t

Example: a = 899, b=493

899 = 1·493 + 406

493 = 1·406 + 87

406 = 4·87 + 58

87 = 1·58 + 29

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

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 – 58
= -6·899 + 11·493

58 = 2·29 + 0 done, gcd = 29

s = -6, t = 11

the Pulverizer

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)

Generalized Die Hard

Did it with buckets:

3 gal. & 5 gal.

3 gal. & 9 gal.

Now a gal. and b gal.?

Generalized Die Hard

Can get *any* linear combination of a, b in a Die Hard bucket (if there's room for it).

Namely, say $0 \le sa + tb < b$.

Get sa +tb into the b gal. bucket as follows:

Generalized Die Hard

assume s > 0. do s times:

- fill bucket *a*, pour into *b*
  -- if b fills, empty it.

total poured = sa

$0 \le$ amount left $\le$ b

times b emptied must be -t

Generalized Die Hard

In fact, no need to count:

- fill bucket a, pour into *b*
  -- if b fills, empty it.

until desired amount is in b !

Team Problems

Problems 1—3