

6	9	13	7
12	10	5	
3	1	4	14
15	8	11	2

Mathematics for Computer Science

MIT 6.042J/18.062J

Intro to Number Theory: Divisibility, GCD's

Copyright © Albert R. Meyer, 2007. All rights reserved.

March 21, 2007

lec 7W.1

6	9	13	7
12	10	5	
3	1	4	14
15	8	11	2

Arithmetic Assumptions

Algebraic rules for $+$, $-$, \times :

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

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

$$a + 0 = a, \quad a+1 > a, \dots$$

We take these for granted!

Copyright © Albert R. Meyer, 2007. All rights reserved.

March 21, 2007

lec 7W.2

6	9	13	7
12	10	5	
3	1	4	14
15	8	11	2

Divisibility

a "divides" b ($a|b$):

$$b = ak \text{ for some } k$$

$$5|15 \text{ because } 15 = 3 \cdot 5$$

$$n|0 \text{ because } 0 = n \cdot 0$$

Copyright © Albert R. Meyer, 2007. All rights reserved.

March 21, 2007

lec 7W.3

6	9	13	7
12	10	5	
3	1	4	14
15	8	11	2

Simple Divisibility Facts

$$a|b \text{ implies } a|bc$$

$$a|b \text{ and } b|c \text{ implies } a|c$$

$$a|b \text{ iff } ac|bc$$

$$\text{for } c \neq 0$$

Copyright © Albert R. Meyer, 2007. All rights reserved.

March 21, 2007

lec 7W.4

6	9	13	7
12	10	5	
3	1	4	14
15	8	11	2

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 .

Copyright © Albert R. Meyer, 2007. All rights reserved.

March 21, 2007

lec 7W.5

6	9	13	7
12	10	5	
3	1	4	14
15	8	11	2

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 .

Copyright © Albert R. Meyer, 2007. All rights reserved.

March 21, 2007

lec 7W.6

6	9	10	7
12	10	5	
3	1	4	14
15	8	11	2

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

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

Copyright © Albert R. Meyer, 2007. All rights reserved.

March 21, 2007

lec 7W.7

6	9	10	7
12	10	5	
3	1	4	14
15	8	11	2

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 .

Copyright © Albert R. Meyer, 2007. All rights reserved.

March 21, 2007

lec 7W.8

6	9	10	7
12	10	5	
3	1	4	14
15	8	11	2

The Division Theorem

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

$q ::= \text{quotient}(a,b)$,

$r ::= \text{remainder}(a,b)$, such that

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

Take this for granted too!

Copyright © Albert R. Meyer, 2007. All rights reserved.

March 21, 2007

lec 7W.11

6	9	10	7
12	10	5	
3	1	4	14
15	8	11	2

Corollary

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

$$a = qb + r, \text{ so}$$

$$r = (-q) \cdot b + 1 \cdot a$$

Copyright © Albert R. Meyer, 2007. All rights reserved.

March 21, 2007

lec 7W.12

6	9	10	7
12	10	5	
3	1	4	14
15	8	11	2

GCD is a linear combination

Theorem: $\text{gcd}(a,b)$ is the smallest positive linear combination of a and b .

$$\text{spc}(a,b)$$

Copyright © Albert R. Meyer, 2007. All rights reserved.

March 21, 2007

lec 7W.13

6	9	10	7
12	10	5	
3	1	4	14
15	8	11	2

1st show: $\text{gcd}(a,b) \leq \text{spc}(a,b)$

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

$$\text{gcd}(a,b) \mid \text{spc}(a,b).$$

In particular,

$$\text{gcd}(a,b) \leq \text{spc}(a,b).$$

Copyright © Albert R. Meyer, 2007. All rights reserved.

March 21, 2007

lec 7W.14

6	9	10	7
12	10	5	
3	5	14	4
15	8	11	2

2nd: $\text{spc}(a,b) \leq \text{gcd}(a,b)$

Enough to show that $\text{spc}(a,b)$ is a common divisor of *just* a .

Copyright © Albert R. Meyer, 2007. All rights reserved.

March 21, 2007

lec 7W.15

6	9	10	7
12	10	5	
3	5	14	4
15	8	11	2

Lemma: $\text{spc}(a,b) \mid a$

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

Copyright © Albert R. Meyer, 2007. All rights reserved.

March 21, 2007

lec 7W.16

6	9	10	7
12	10	5	
3	5	14	4
15	8	11	2

Prime Divisibility

Lemma: p prime and $p \mid a \cdot b$ implies $p \mid a$ or $p \mid b$.

pf: say $\neg(p \mid a)$. so $\text{gcd}(p,a)=1$.

$$\begin{aligned} \text{so, } sa + tp &= 1 \\ (sa)b + (tp)b &= b \\ \underbrace{sa}_p \underbrace{b}_p + \underbrace{tp}_p \underbrace{b}_p &= b \\ p \mid p \mid \text{so } p \mid b \end{aligned}$$

QED

Copyright © Albert R. Meyer, 2007. All rights reserved.

March 21, 2007

lec 7W.17

6	9	10	7
12	10	5	
3	5	14	4
15	8	11	2

Prime Divisibility

Cor: If p is prime, and $p \mid a_1 \cdot a_2 \cdots a_m$

then $p \mid a_i$ for some i .

pf: By induction on m .

Copyright © Albert R. Meyer, 2007. All rights reserved.

March 21, 2007

lec 7W.18

6	9	10	7
12	10	5	
3	5	14	4
15	8	11	2

Finding s and t

Given a,b , how to find s,t so that $sa+tb=\text{gcd}(a,b)$?

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

Copyright © Albert R. Meyer, 2007. All rights reserved.

March 21, 2007

lec 7W.19

6	9	10	7
12	10	5	
3	5	14	4
15	8	11	2

Finding s and t

Example: $a = 899, b = 493$

$$899 = 1 \cdot 493 + 406$$

$$493 = 1 \cdot 406 + 87$$

$$406 = 4 \cdot 87 + 58$$

$$87 = 1 \cdot 58 + 29$$

$$58 = 2 \cdot 29 + 0$$

done, $\text{gcd} = 29$

Copyright © Albert R. Meyer, 2007. All rights reserved.

March 21, 2007

lec 7W.20

6	9	10	7
12	10	5	
3	4	14	
15	8	11	2

Finding s and t

Example: $a = 899$, $b = 493$

$$\begin{aligned} 899 &= 1 \cdot 493 + 406 & \text{so } 406 &= 1 \cdot 899 + -1 \cdot 493 \\ 493 &= 1 \cdot 406 + 87 & \text{so } 87 &= 493 - 1 \cdot 406 \\ & & &= -1 \cdot 899 + 2 \cdot 493 \\ 406 &= 4 \cdot 87 + 58 & \text{so } 58 &= 406 - 4 \cdot 87 \\ & & &= 5 \cdot 899 + -9 \cdot 493 \\ 87 &= 1 \cdot 58 + 29 & \text{so } 29 &= 87 - 1 \cdot 58 \\ & & &= -6 \cdot 899 + 11 \cdot 493 \\ 58 &= 2 \cdot 29 + 0 & \text{done, gcd} &= 29 \end{aligned}$$

Copyright © Albert R. Meyer, 2007. All rights reserved.

March 21, 2007

lec 7W.21

6	9	10	7
12	10	5	
3	4	14	
15	8	11	2

Finding s and t

Example: $a = 899$, $b = 493$

$$\begin{aligned} 899 &= 1 \cdot 493 + 406 & \text{so } 406 &= 1 \cdot 899 + -1 \cdot 493 \\ 493 &= 1 \cdot 406 + 87 & \text{so } 87 &= 493 - 1 \cdot 406 \\ & & &= -1 \cdot 899 + 2 \cdot 493 \\ 406 &= 4 \cdot 87 + 58 & \text{so } 58 &= 406 - 4 \cdot 87 \\ & & &= 5 \cdot 899 + -9 \cdot 493 \\ 87 &= 1 \cdot 58 + 29 & \text{so } 29 &= 87 - 1 \cdot 58 \\ & & &= -6 \cdot 899 + 11 \cdot 493 \\ 58 &= 2 \cdot 29 + 0 & \text{done, gcd} &= 29 \\ & & & \mathbf{s = -6, t = 11} \end{aligned}$$

the Pulverizer

Copyright © Albert R. Meyer, 2007. All rights reserved.

March 21, 2007

lec 7W.22

6	9	10	7
12	10	5	
3	4	14	
15	8	11	2

Finding $s > 0$ and t

$$\begin{aligned} \text{gcd}(899, 493) &= -6 \cdot 899 + 11 \cdot 493 \\ \text{get positive coeff. for } 899? & \\ (-6 + 493k) \cdot 899 + (11 - 899k) \cdot 493 & \\ = -6 \cdot 899 + 11 \cdot 493 & \\ \text{so use } k=1: 487 \cdot 899 + -888 \cdot 493 & \\ = \text{gcd}(899, 493) & \end{aligned}$$

Copyright © Albert R. Meyer, 2007. All rights reserved.

March 21, 2007

lec 7W.23

6	9	10	7
12	10	5	
3	4	14	
15	8	11	2

Generalized Die Hard

Did it with buckets:

3 gal. & 5 gal.

3 gal. & 9 gal.

Now a gal. and b gal.?

Copyright © Albert R. Meyer, 2007. All rights reserved.

March 21, 2007

lec 7W.24

6	9	10	7
12	10	5	
3	4	14	
15	8	11	2

Generalized Die Hard

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

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

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

Copyright © Albert R. Meyer, 2007. All rights reserved.

March 21, 2007

lec 7W.26

6	9	10	7
12	10	5	
3	4	14	
15	8	11	2

Generalized Die Hard

assume $s > 0$. do s times:

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

total poured = sa

$0 \leq \text{amount left} \leq b$

times b emptied must be $-t$

Copyright © Albert R. Meyer, 2007. All rights reserved.

March 21, 2007

lec 7W.27



1	2	3
4	5	6
7	8	9

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* !

Copyright © Albert R. Meyer, 2007. All rights reserved.

March 21, 2007

lec 7W.28



1	2	3
4	5	6
7	8	9

Team Problems

Problems 1—3

Copyright © Albert R. Meyer, 2007. All rights reserved.

March 21, 2007

lec 7W.35