

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

Mathematics for Computer Science

MIT 6.042J/18.062J

Prime Factorization Congruences

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

April 2, 2007

lec 8M.1

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

Prime Divisibility

Lemma: If p is prime, and
 $p \mid a \cdot b$,

then $p \mid a$ or $p \mid b$.

pf: in earlier lecture. follows from

$$\gcd(p, a) = xa + yp$$

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

April 2, 2007

lec 8M.3

6	9	13	7
12	10	5	
3	1	4	14
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.

April 2, 2007

lec 8M.4

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

Unique Prime Factorization

Fundamental Theorem of Arithmetic

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

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

April 2, 2007

lec 8M.5

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

Unique Prime Factorization

Fundamental Theorem of Arithmetic

Example:

$$61394323221 =$$

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

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

April 2, 2007

lec 8M.6

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

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 $q_1 \neq p_i$ all i

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

April 2, 2007

lec 8M.7

6	9	10	7
12	18	5	
3	1	4	14
15	8	11	2

Unique Prime Factorization

pf: $n = p_1 \cdot p_2 \cdots p_k = q_1 \cdot q_2 \cdots q_m$
 now $p_1 | n$, so by Cor., $p_1 | q_i$.
 so $p_1 = q_i$ with $i > 1$.
 so $\underbrace{p_2 \cdots p_k}_{< n} = q_1 \cdot q_2 \cdots q_{i-1} \cdot q_{i+1} \cdots q_m$
 and $q_1 \neq p_2$

contradiction!

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

April 2, 2007

lec 8M.8

6	9	10	7
12	18	5	
3	1	4	14
15	8	11	2

Unique Prime Factorization

Cor: if $n = p_1 \cdot p_2 \cdots p_k$,
 and $m | n$, then

$$m = p_{i_1} \cdot p_{i_2} \cdots p_{i_j}$$

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

April 2, 2007

lec 8M.9

6	9	10	7
12	18	5	
3	1	4	14
15	8	11	2

Team Problem

Problem 1

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

April 2, 2007

lec 8M.10

6	9	10	7
12	18	5	
3	1	4	14
15	8	11	2

Congruences

Def: $a \equiv b \pmod{n}$ iff $n | (a - b)$.

Lemma: If $a \equiv b \pmod{n}$, then
 $a + c \equiv b + c \pmod{n}$.

pf: $n | (a - b)$ implies
 $n | ((a + c) - (b + c))$

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

April 2, 2007

lec 8M.11

6	9	10	7
12	18	5	
3	1	4	14
15	8	11	2

Congruences

Lemma:

If $a \equiv b \pmod{n}$, then
 $a \cdot c \equiv b \cdot c \pmod{n}$.

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

April 2, 2007

lec 8M.13

6	9	10	7
12	18	5	
3	1	4	14
15	8	11	2

Congruences

Lemma:

$$a \equiv \text{rem}(a, n) \pmod{n}$$

important: keeps (mod n)
 calculations in the range
 0 to n-1

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

April 2, 2007

lec 8M.14

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

Congruences

Cor: $a \equiv b \pmod{n}$ iff
 $\text{rem}(a,n) = \text{rem}(b,n)$

Cor: $a \equiv a \pmod{n}$.

If $a \equiv b$ & $b \equiv c \pmod{n}$,
 then $a \equiv c \pmod{n}$

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

April 2, 2007

lec 8M.15

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

Congruences

So $\equiv \pmod{n}$ a lot like $=$.

main diff: can't cancel

$$4 \cdot 2 \equiv 1 \cdot 2 \pmod{6}$$

$$4 \not\equiv 1 \pmod{6}$$

No general cancellation

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

April 2, 2007

lec 8M.16

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

Relatively prime cancellation

If $\text{gcd}(k,n)=1$, then have k'
 $k \cdot k' \equiv 1 \pmod{n}$.

k' is an *inverse* mod n of k

pf: $sk + tn = 1$.

just let $k' = s$.

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

April 2, 2007

lec 8M.17

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

Relatively prime cancellation

Cor.

If $i \cdot k \equiv j \cdot k \pmod{n}$,

and $\text{gcd}(k,n) = 1$,

then $i \equiv j \pmod{n}$

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

April 2, 2007

lec 8M.18

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

Fermat's Little Theorem

If p is prime & k not a multiple of p ,
 can cancel k . So

$$k, 2k, \dots, (p-1)k$$

are all different \pmod{p} .

So their remainders on division
 by p are all different \pmod{p} .

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

April 2, 2007

lec 8M.19

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

Fermat's Little Theorem

This means that

$\text{rem}(k, p), \text{rem}(2k, p), \dots, \text{rem}((p-1)k, p)$

must be a *permutation* of

$$1, 2, \dots, (p-1)$$

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

April 2, 2007

lec 8M.20

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

Fermat's Little Theorem

so $1 \cdot 2 \cdots (p-1) =$

$\text{rem}(k,p) \cdot \text{rem}(2k,p) \cdots \text{rem}((p-1)k,p)$

$\equiv (k) \cdot (2k) \cdots ((p-1)k) \pmod{p}$

$\equiv (k^{p-1}) \cdot 1 \cdot 2 \cdots (p-1) \pmod{p}$

so

$$1 \equiv k^{p-1} \pmod{p}$$

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

April 2, 2007

lec 8M.21

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

Team Problems

Problems 2–4

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

April 2, 2007

lec 8M.22