

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

Mathematics for Computer Science  
MIT 6.042J/18.062J

## Cancellation & Inverses (mod n)



Albert R Meyer, March 9, 2015

inversemodn.1

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

## Congruence mod n

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



Albert R Meyer, March 9, 2015

inversemodn.2

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

## Congruence mod n

So arithmetic (mod n) a lot  
like ordinary arithmetic

the main difference:

$$8 \cdot \cancel{2} \equiv 3 \cdot \cancel{2} \pmod{10}$$

$$8 \not\equiv 3 \pmod{10}$$

**no arbitrary cancellation**



Albert R Meyer, March 9, 2015

inversemodn.3

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

## cancellation (mod n)

When can you cancel  $k$ ?  
—when  $k$  has no common  
factors with  $n$



Albert R Meyer, March 9, 2015

inversemodn.4

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

## inverses (mod n)

If  $\gcd(k,n)=1$ , then have  $k'$

$$k' \cdot k \equiv 1 \pmod{n}.$$

$k'$  is an **inverse** mod  $n$  of  $k$

pf:  $sk + tn = 1$ , so

just let  $k'$  be  $s$



Albert R Meyer, March 9, 2015

inversemodn.5

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

## inverses (mod n)

$$sk + tn = 1$$

$$sk + tn \equiv 1 \pmod{n}$$

$$sk + t0 \equiv 1 \pmod{n}$$

$$sk \equiv 1 \pmod{n}$$

so  $s$  is an inverse of  $k$



Albert R Meyer, March 9, 2015

inversemodn.6

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

## cancellation (mod n)

If  $a \cdot k \equiv b \cdot k \pmod{n}$

and  $\gcd(k,n) = 1$ , then

multiply by  $k'$ :

$$(a \cdot k) \cdot k' \equiv (b \cdot k) \cdot k' \pmod{n}$$

$$a \cdot 1 \equiv b \cdot 1$$

so  $a \equiv b \pmod{n}$



Albert R Meyer, March 9, 2015

inversemodn.7

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

## cancellation (mod n)

summary:

$k$  is **cancellable** (mod  $n$ ) iff

$k$  has an **inverse** (mod  $n$ ) iff

$k$  is **relatively prime** to  $n$



Albert R Meyer, March 9, 2015

inversemodn.8