

# Modular arithmetic

---

Linguistics 484

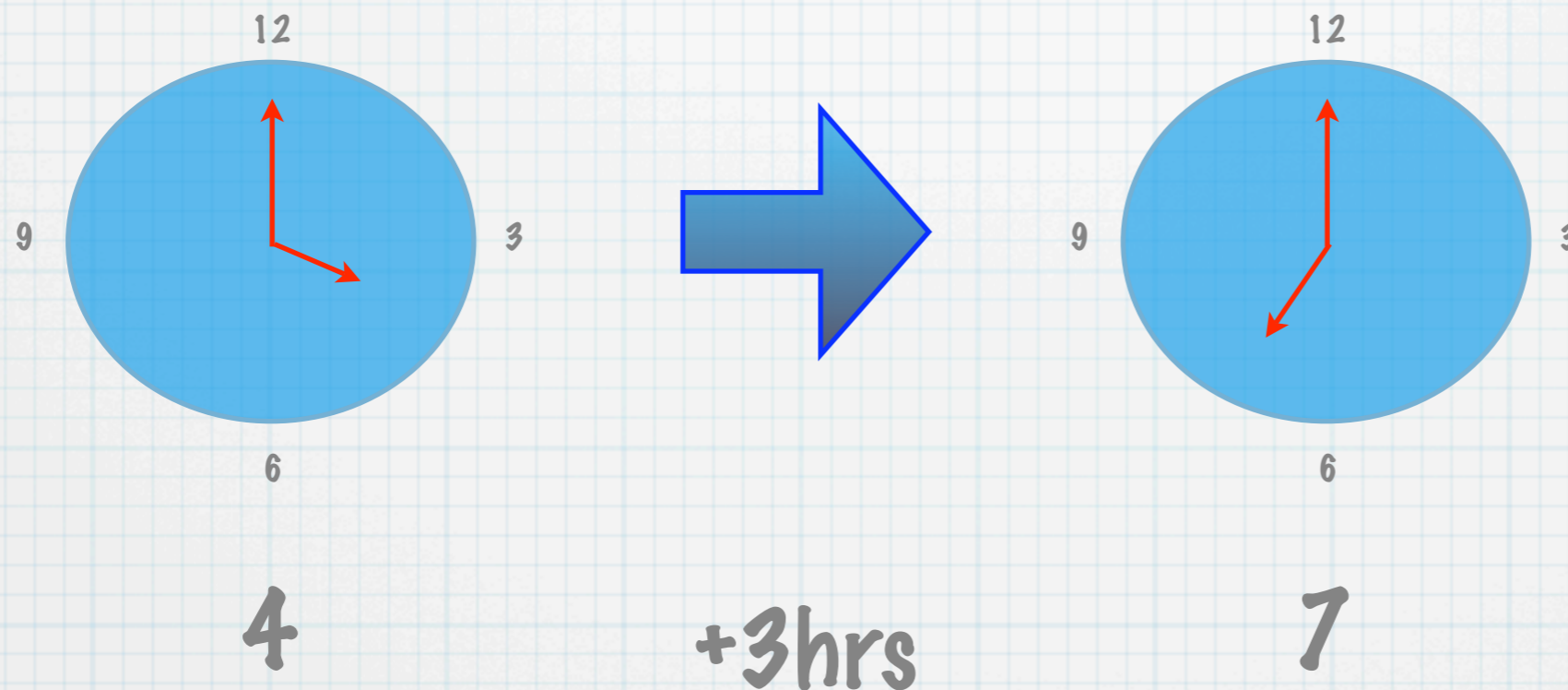
# From last time

- \* Multiplication mod 26 doesn't always produce a workable code
- \* Specifically,
  - \* 3,5,7,9,11,15,17,19,21,23,25 all work
  - \* 2,4,6,8,10,12,13,14,16,18,20,22,24,26 all collapse alphabet onto too few slots

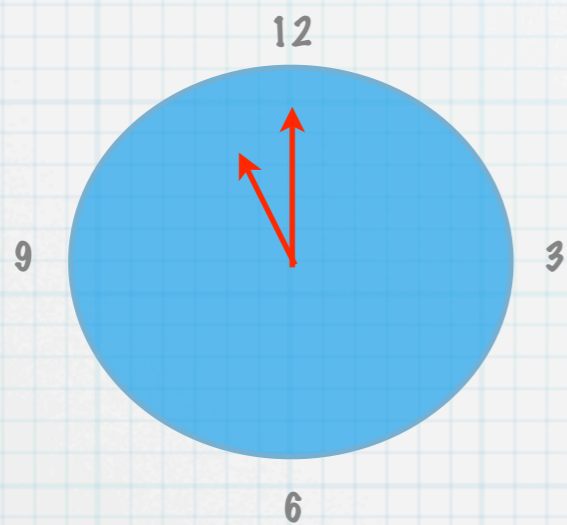
# What's going on?

- \* Review of modular arithmetic
- \* Euclid's algorithm
- \*

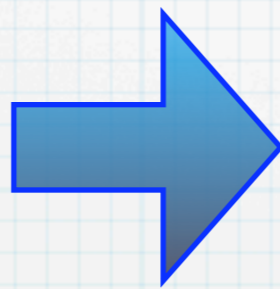
# Clock arithmetic



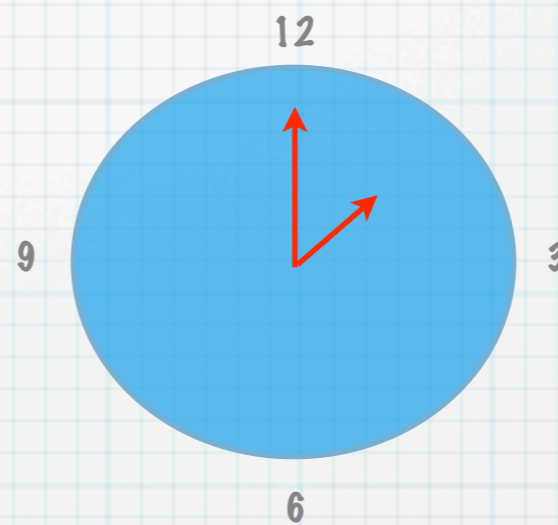
# Clock arithmetic



11

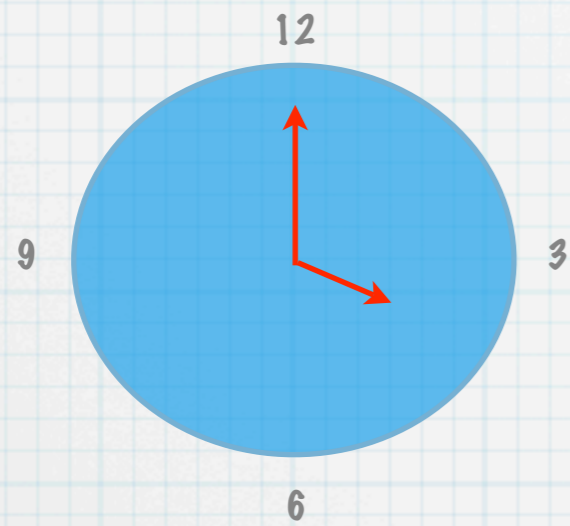


+3hrs

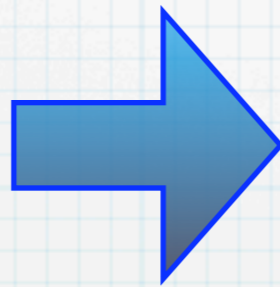


2

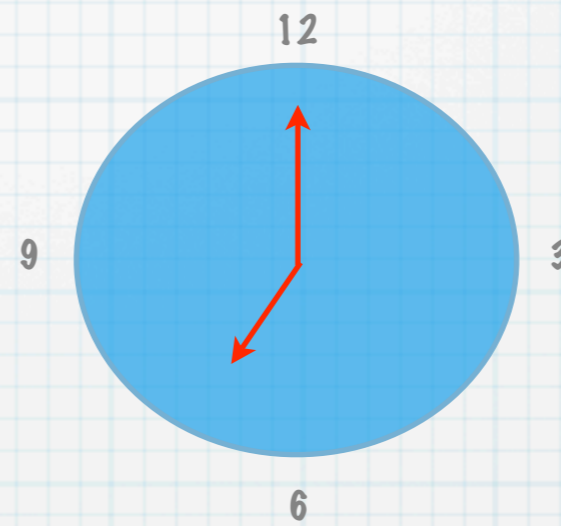
# Military time



16

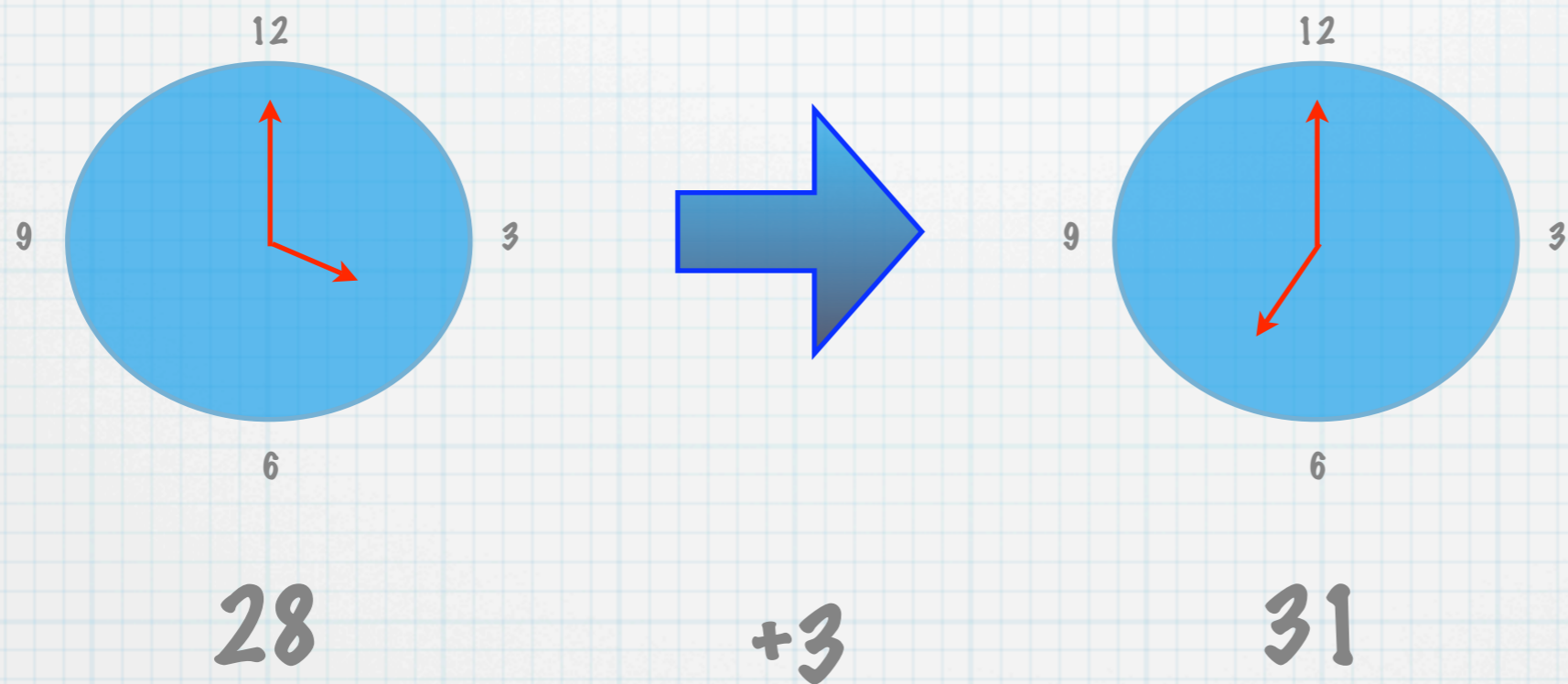


+3



19

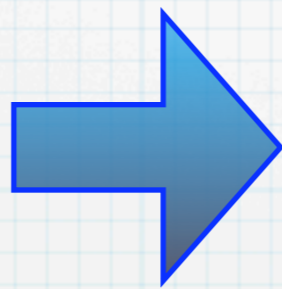
# Hypermilitary



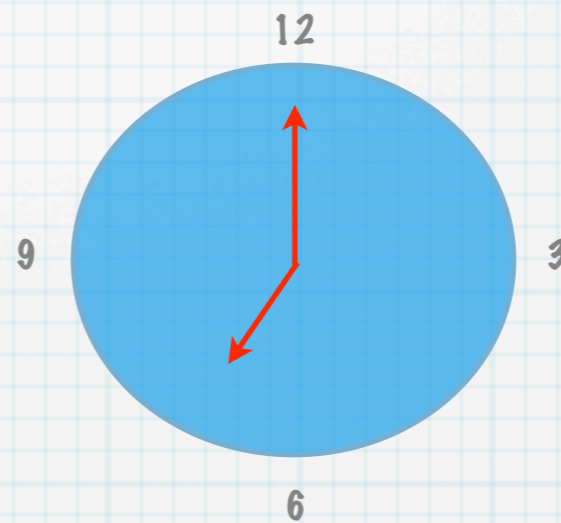
# Tidy up



$$28-24=4$$

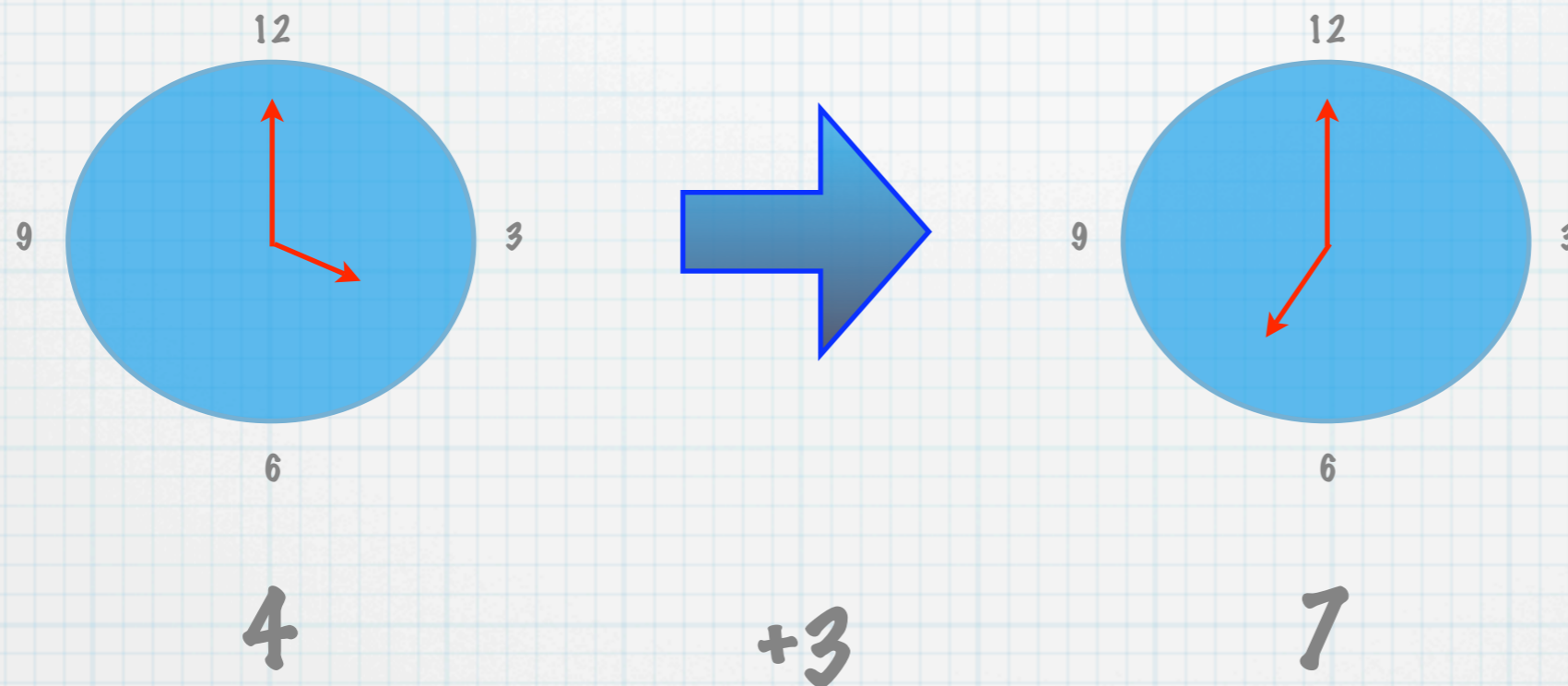


$$+3$$

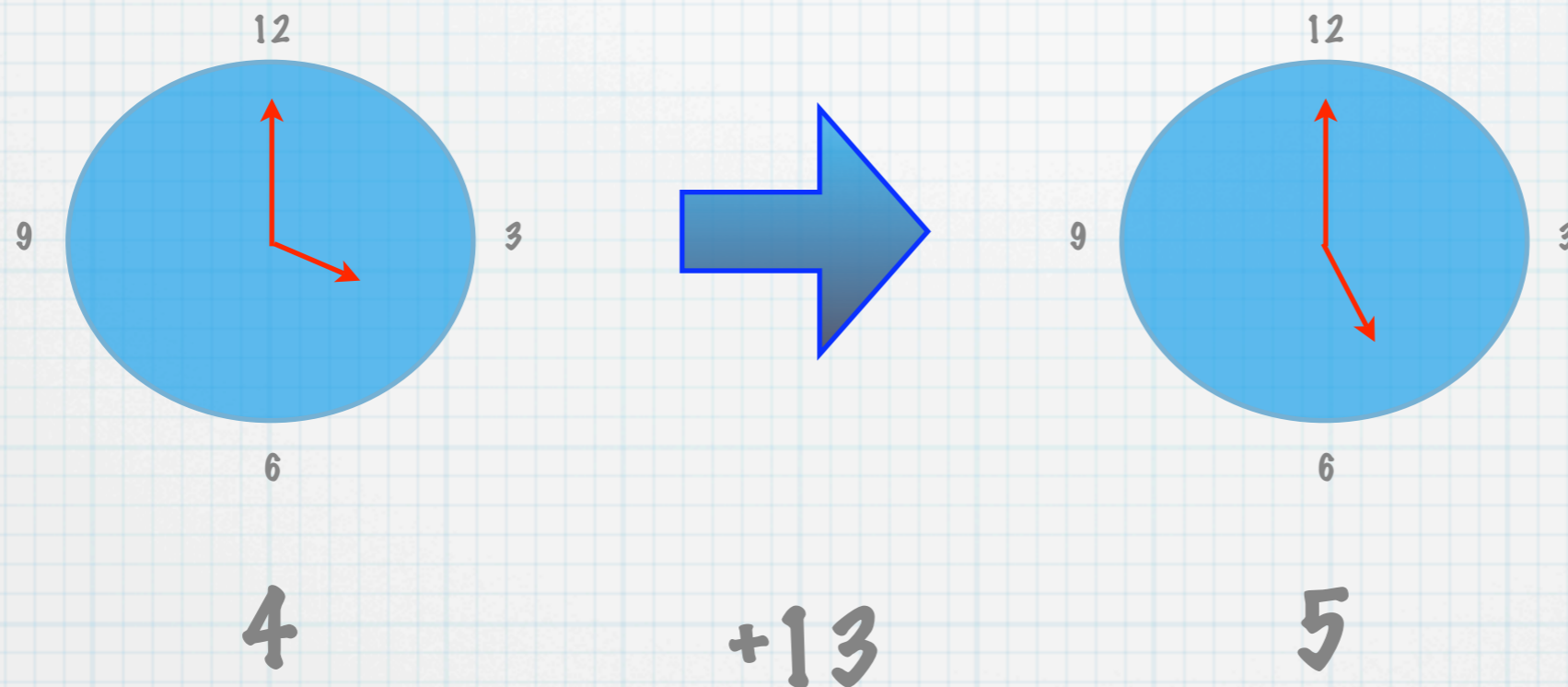


$$31-24=7$$

# Modular arithmetic (mod 12)



# Modular arithmetic (mod 12)



# More on modular arithmetic

- \* We write  $x \equiv y \pmod{p}$  to indicate that two numbers  $x$  and  $y$  are equivalent in arithmetic modulo  $p$ .
- \* Imagine a clock face with  $p$  numbers. Two numbers are equivalent if they point at the same place on the clock face.

# Arithmetic

- \*  $x \equiv y \pmod{p}$  if there exist integers  $a$  and  $b$  such that  $x = a \cdot p + r$  and  $y = b \cdot p + r$  where  $r < p$ .
- \* In other words, if  $x$  corresponds to going round a  $p$ -sized clock  $a$  times then  $r$  more, and  $y$  corresponds to going round a  $p$ -sized clock  $b$  times then  $r$  more.

# Modular inverse

- \* Solve for  $m*n \equiv 1 \pmod{p}$ .
- \* In other words, you win if you start at 0, do a jump of  $x$  units  $y$  times on a  $p$ -sized clock and land on 1.
- \* It would be just as good to solve  $m*n + y*p \equiv 1$  (in regular arithmetic)

# Example

\* Solve  $14x + 10 = 8 \pmod{9}$ .

# Example

- \* Solve  $14x + 10 \equiv 8 \pmod{9}$ .
- \*  $14x \equiv -2 \pmod{9}$ , subtract 10
- \*  $14x \equiv 7 \pmod{9}$       $-2 \equiv 7 \pmod{9}$
- \*  $5x \equiv 7 \pmod{9}$       $14 \equiv 5 \pmod{9}$
- \* Try  $x = 1, 2, 3, 4, 5, 6, 7, 8, 9$

# Example

\* Solve  $14^*x+10 \equiv 8 \pmod{9}$ .

\* ... Answer:  $x = 5$

\* Check:  $14^*x = 70 + 10 = 80 = 72+8 =$   
 $(8^*9)+8 = 8 \pmod{9}$

# In class exercises

December 2008

Su	M	T	W	Th	F	Sa
30	1	2	3	4	5	6
7	8	9	10	11	12	13
14	15	16	17	18	19	20
21	22	23	24	25	26	27
28	19	30	31	1	2	3

What day of the week is congruent to  $3 \pmod{7}$  in December 2008?

# In class exercises

December 2008

Su	M	T	W	Th	F	Sa
30	1	2	3	4	5	6
7	8	9	10	11	12	13
14	15	16	17	18	19	20
21	22	23	24	 25	26	27
28	19	30	31	1	2	3

What day of the week is congruent to  $3 \pmod{7}$  in December 2008?

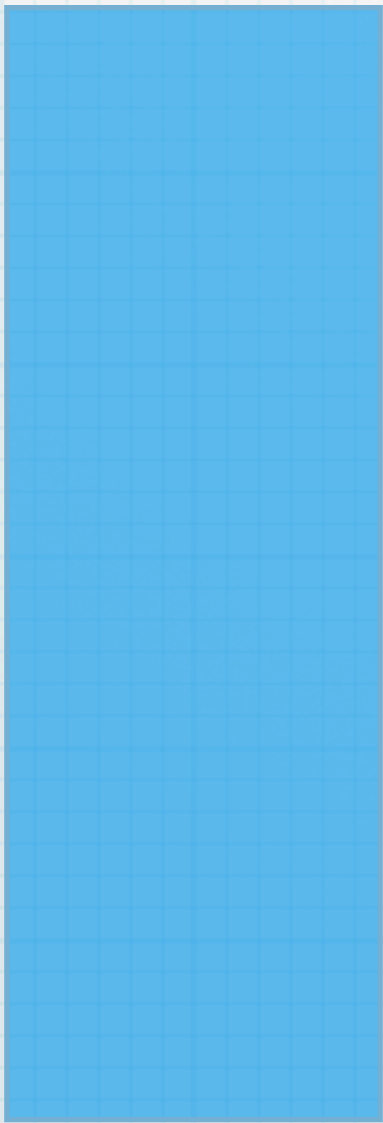
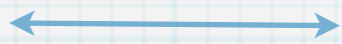
# In class exercises

- \* Solve  $x+12 \equiv 3 \pmod{5}$ .
- \* Solve  $y-1 \equiv 13 \pmod{6}$ .

# Euclid's algorithm

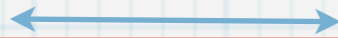
- \* Apparent diversion, but not really
- \* Find Greatest Common Divisor of two numbers
- \* One of the oldest known algorithms

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



$a$

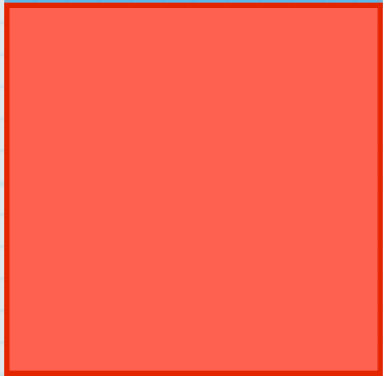
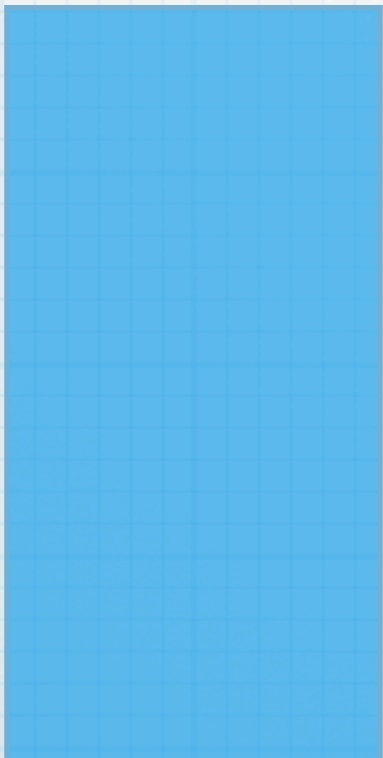
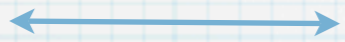
$\text{gcd}(a,b)$



$b$

Arrange boxes with  
width =  $\text{gcd}(a,b)$

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



$a$

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

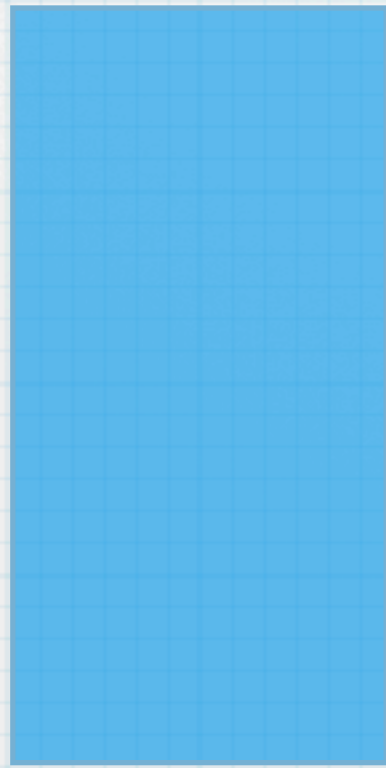


$b$



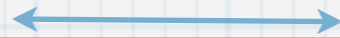
Arrange boxes with  
width =  $\text{gcd}(a,b)$

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



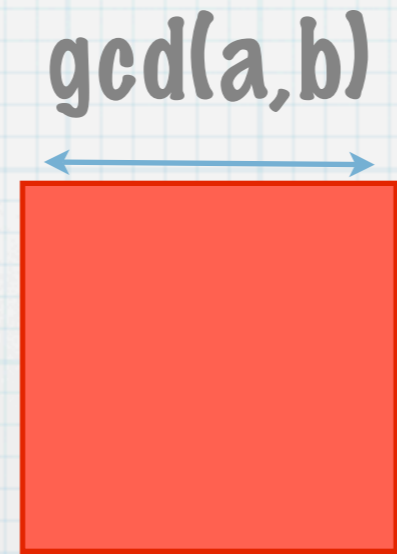
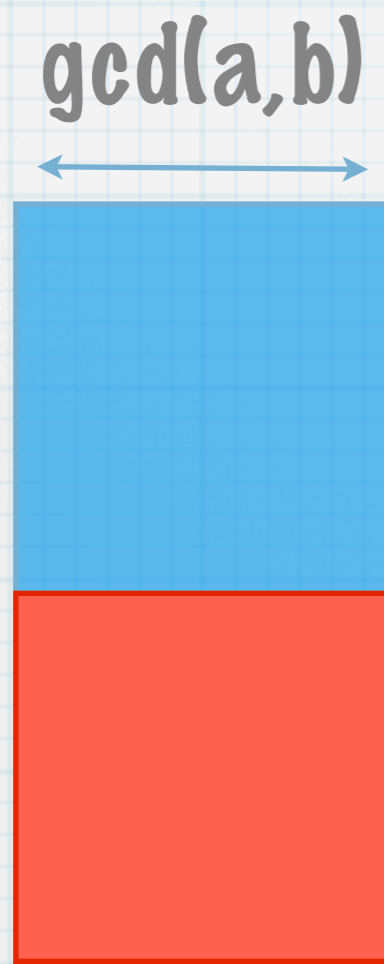
$a$

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



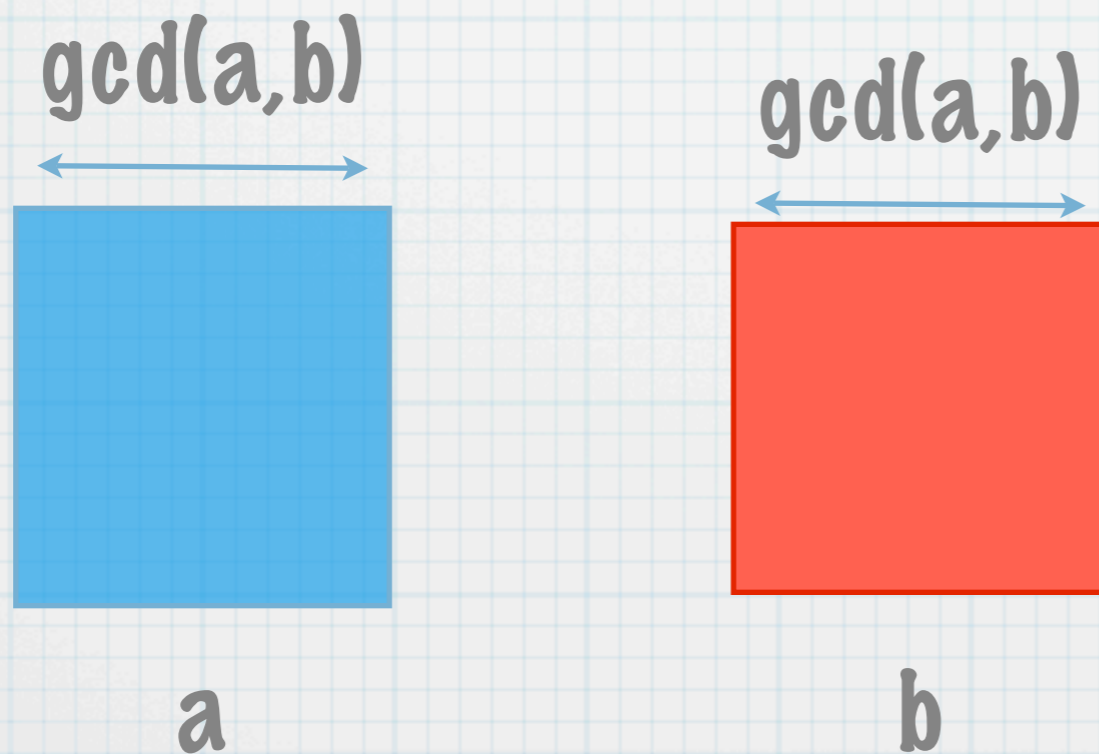
$b$

Arrange boxes with  
width =  $\text{gcd}(a,b)$

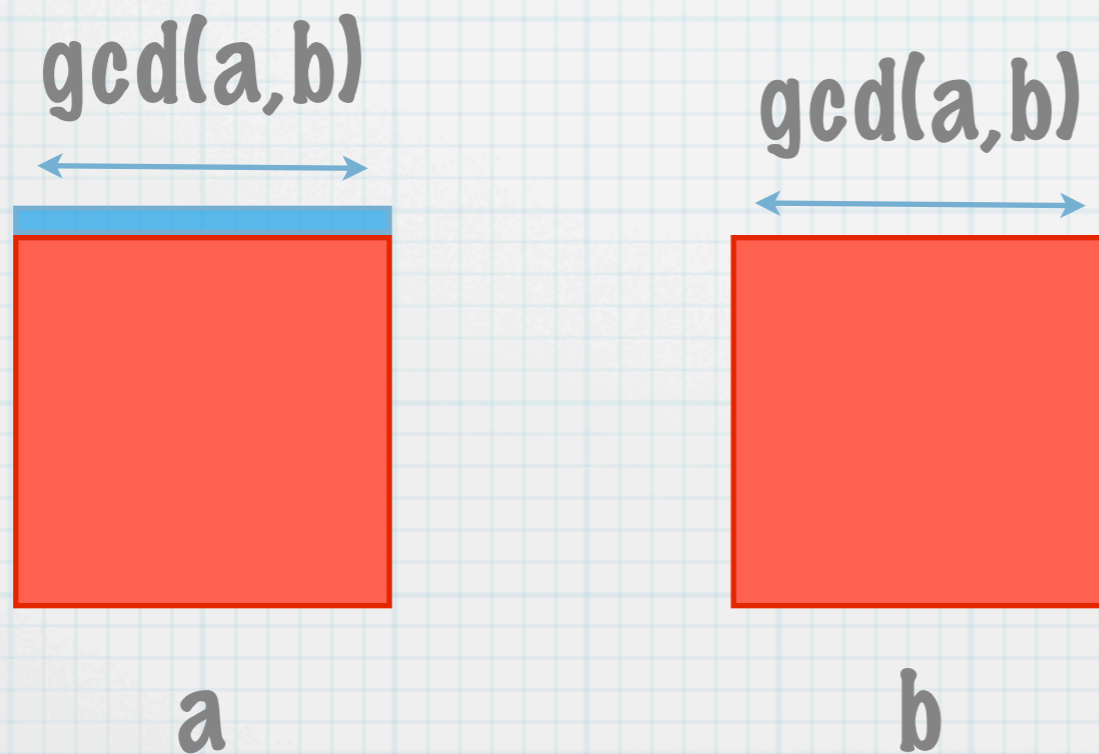


Arrange boxes with  
width =  $\text{gcd}(a,b)$

Arrange boxes with  
width =  $\text{gcd}(a,b)$



Arrange boxes with  
width =  $\text{gcd}(a,b)$



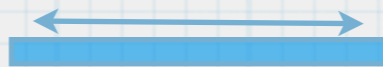
Arrange boxes with  
width =  $\text{gcd}(a,b)$

$\text{gcd}(a,b)$   
←→



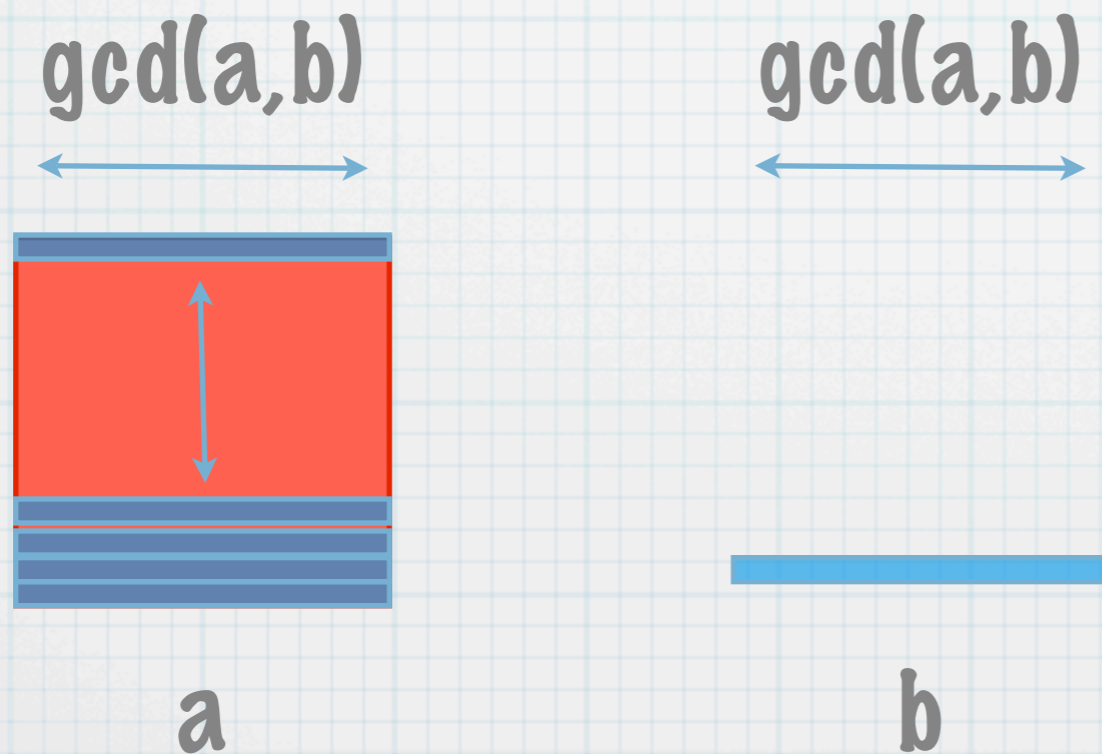
a

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



b

Diagram shows multiple steps and b fits inside a with no overlap



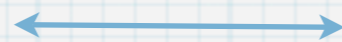
Hopefully obvious that  
this is correct.

$\gcd(a,b)$



$a$

$\gcd(a,b)$



$b$