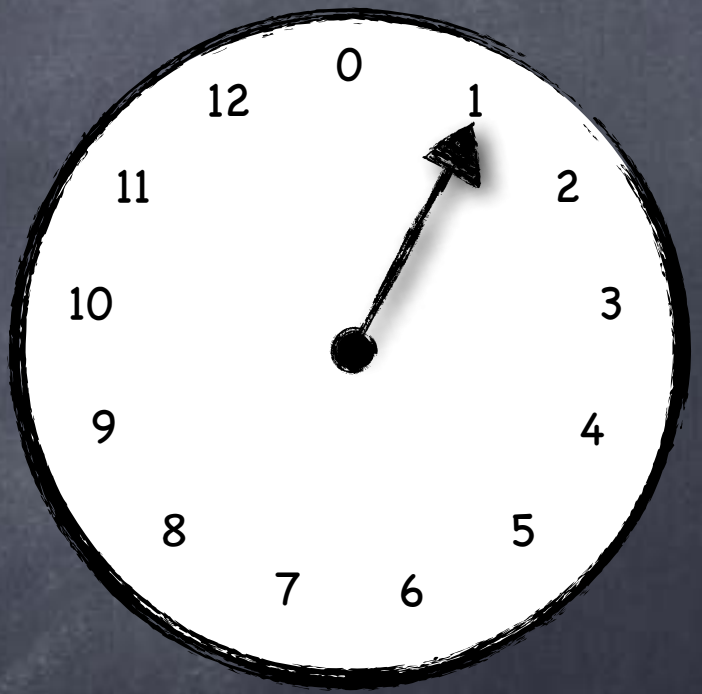
# Numb3rs

## Modular Arithmetic



# Congruence

- For a "modulus" m and two integers a and b, we say $a \equiv b \pmod{m}$ if $m \mid (a-b)$

- Typically, we shall consider modulus > 0
  - $a \equiv b \pmod{0} \leftrightarrow a=b$
  - $a \equiv b \pmod{1}$
  - $a \equiv b \pmod{m} \leftrightarrow a \equiv b \pmod{|m|}$

# Quotient-Remainder Theorem

For any two integers m and n, m≠0, there is a unique quotient q and remainder r (integers), such that

$$n = q \cdot m + r, \quad 0 \le r < |m|$$

rem(n,m)

m=7

| q | | | | | | | |
|---|---|---|---|---|---|---|---|
| -2 | -14 | -13 | -12 | -11 | -10 | -9 | -8 |
| -1 | -7 | -6 | -5 | -4 | -3 | -2 | -1 |
| | 0 | 1 | 2 | 3 | 4 | 5 | 6 |
| 0 | 0 | 1 | 2 | 3 | 4 | 5 | 6 |
| 1 | 7 | 8 | 9 | 10 | 11 | 12 | 13 |
| 2 | 14 | 15 | 16 | 17 | 18 | 19 | 20 |

r

# Congruence

- For a "modulus" m and two integers a and b, we say $a \equiv b \pmod{m}$ if $m|(a-b)$

- Claim: $a \equiv b \pmod{m}$ iff $rem(a,m) = rem(b,m)$
- Proof: Let $rem(a,m) = r_1$, $rem(b,m) = r_2$.
  Let $a = q_1 m + r_1$ and $b = q_2 m + r_2$.
  Then $a-b = (q_1-q_2)m + (r_1-r_2)$.
  - $a-b=qm \Rightarrow (r_1-r_2) = q'm$. $r_1, r_2 \in [0,m) \Rightarrow |r_1-r_2| < m \Rightarrow r_1=r_2$
  - $r_1=r_2 \Rightarrow a-b=qm$ where $q=q_1-q_2$.

# Congruence

For a "modulus" m and two integers a and b, we say $a \equiv b \pmod{m}$ if $m|(a-b)$

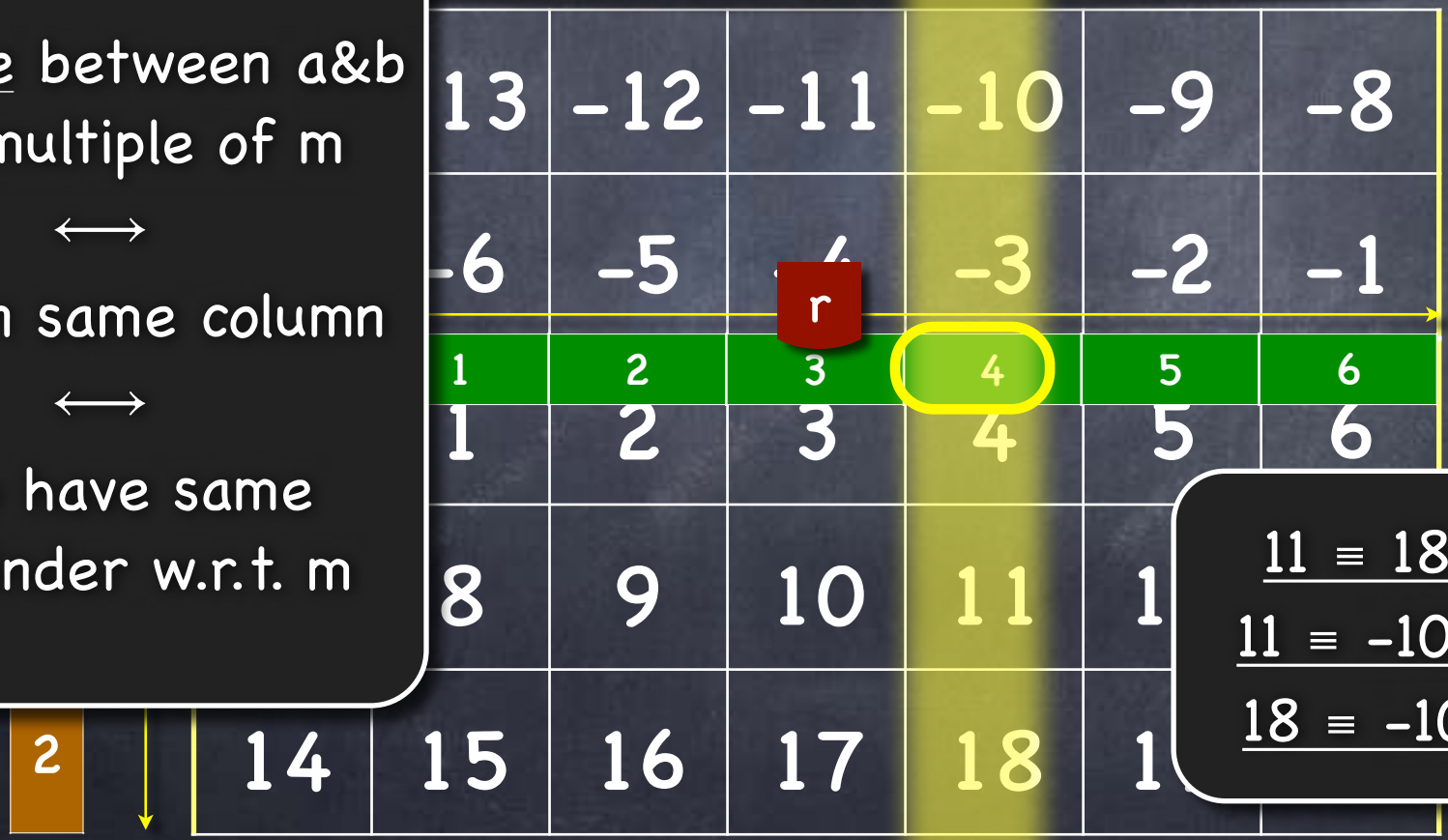
distance between a&b is a multiple of m

$\longleftrightarrow$

a&b on same column

$\longleftrightarrow$

a&b have same remainder w.r.t. m




$11 \equiv 18 \pmod{7}$

$11 \equiv -10 \pmod{7}$

$18 \equiv -10 \pmod{7}$

# Modular Arithmetic

- Fix a modulus m.
  Elements of the universe: columns in the "table" for m
- Let $[a]_m$ stand for the column containing a
  - i.e., stands for all elements x, s.t. $a \equiv x \pmod{m}$
  - e.g.: $[-17]_5 = [-2]_5 = [3]_5$
- $\mathbb{Z}_m = \{ [0]_m, \ldots, [m-1]_m \}$ (or simply, $\{0,\ldots,m-1\}$)
- We shall define operations in $\mathbb{Z}_m$, i.e., among the columns

# Modular Addition

- $[a]_m$ : the set of all elements x, s.t. $a \equiv x \pmod m$
- Modular addition: $[a]_m +_m [b]_m \triangleq [a+b]_m$
  - Well-defined? Or, are we defining the same element to have two different values?
  - $\underline{[a]_m = [a']_m} \wedge \underline{[b]_m = [b']_m} \rightarrow \underline{[a+b]_m = [a'+b']_m}$ ?
    - i.e., $m|(a-a') \wedge m|(b-b') \rightarrow m|\ ((a+b) - (a'+b'))$ ?
    - $(a+b)-(a'+b') = (a-a') + (b-b')$ ✔

# Modular Addition

- $[a]_m$ : the set of all elements x, s.t. $a \equiv x \pmod m$
- Modular addition: $[a]_m +_m [b]_m \triangleq [a+b]_m$

Inherits various properties of standard addition:
existence of identity and inverse, commutativity, associativity

# Modular Addition

- e.g. m = 6

Every element a has an **additive inverse** -a, so that a + (-a) ≡ 0 (mod m)

| + | 0 | 1 | 2 | 3 | 4 | 5 |
|---|---|---|---|---|---|---|
| 0 | 0 | 1 | 2 | 3 | 4 | 5 |
| 1 | 1 | 2 | 3 | 4 | 5 | 0 |
| 2 | 2 | 3 | 4 | 5 | 0 | 1 |
| 3 | 3 | 4 | 5 | 0 | 1 | 2 |
| 4 | 4 | 5 | 0 | 1 | 2 | 3 |
| 5 | 5 | 0 | 1 | 2 | 3 | 4 |

- e.g. m = 5

| + | 0 | 1 | 2 | 3 | 4 |
|---|---|---|---|---|---|
| 0 | 0 | 1 | 2 | 3 | 4 |
| 1 | 1 | 2 | 3 | 4 | 0 |
| 2 | 2 | 3 | 4 | 0 | 1 |
| 3 | 3 | 4 | 0 | 1 | 2 |
| 4 | 4 | 0 | 1 | 2 | 3 |

More generally, a + x ≡ b (mod m) always has a solution, x = b-a

# Modular Multiplication

- $[a]_m$ : the set of all elements x, s.t. $a \equiv x \pmod m$
- Modular multiplication: $[a]_m \times_m [b]_m \triangleq [a \cdot b]_m$
- $[a]_m = [a']_m \wedge [b]_m = [b']_m \rightarrow [a \cdot b]_m = [a' \cdot b']_m$ ?
  - Suppose $a-a' = pm$, $b-b' = qm$.
  - Then $a \cdot b = (pm+a')(qm+b') = (mpq+pa'+qb')m + a'b'$ ✔

# Modular Multiplication

- $[a]_m$ : the set of all elements x, s.t. $a \equiv x \pmod m$
- Modular multiplication: $[a]_m \times_m [b]_m \triangleq [a \cdot b]_m$

Also commutative, associative

| | | | | | | |
|---|---|---|---|---|---|---|
| -14 | -13 | -12 | -11 | -10 | -9 | -8 |
| -7 | -6 | -5 | -4 | -3 | -2 | -1 |
| 0 | 1 | 2 | 3 | 4 | 5 | 6 |
| 0 | 1 | 2 | 3 | 4 | 5 | 6 |
| 7 | 8 | 9 | 10 | 11 | 12 | 13 |
| 14 | 15 | 16 | 17 | 18 | 19 | 20 |

$-6 \times -3$
$\equiv 18$
$\equiv 1 \times 4$
$\equiv 4 \pmod 7$

identity of multiplication

# Modular Multiplication

- e.g. m = 6

| × | 0 | 1 | 2 | 3 | 4 | 5 |
|---|---|---|---|---|---|---|
| 0 | 0 | 0 | 0 | 0 | 0 | 0 |
| 1 | 0 | 1 | 2 | 3 | 4 | 5 |
| 2 | 0 | 2 | 4 | 0 | 2 | 4 |
| 3 | 0 | 3 | 0 | 3 | 0 | 3 |
| 4 | 0 | 4 | 2 | 0 | 4 | 2 |
| 5 | 0 | 5 | 4 | 3 | 2 | 1 |

Sometimes, the product of two non-zero numbers can be zero!

- e.g. m = 5

| × | 0 | 1 | 2 | 3 | 4 |
|---|---|---|---|---|---|
| 0 | 0 | 0 | 0 | 0 | 0 |
| 1 | 0 | 1 | 2 | 3 | 4 |
| 2 | 0 | 2 | 4 | 1 | 3 |
| 3 | 0 | 3 | 1 | 4 | 2 |
| 4 | 0 | 4 | 3 | 2 | 1 |

Sometimes, a number other than 1 can have a multiplicative inverse!

# Modular Arithmetic

- $[a]_m$ : the set of all elements x, s.t. $a \equiv x \pmod m$
- Modular addition: $[a]_m +_m [b]_m \triangleq [a+b]_m$
- Modular multiplication: $[a]_m \times_m [b]_m \triangleq [a \cdot b]_m$
- Multiplicative Inverse! a has a multiplicative inverse modulo m iff a is co-prime with m.
  - $\gcd(a,m)=1 \leftrightarrow \exists u,v\ au+mv=1 \leftrightarrow \exists u\ [a]_m \times_m [u]_m = [1]_m$
  - e.g. $[2]_9 \times_9 [5]_9 = [1]_9$ so $[2]_9^{-1} = [5]_9$ and $[5]_9^{-1} = [2]_9$
  - For a prime modulus m, all except $[0]_m$ have inverses!