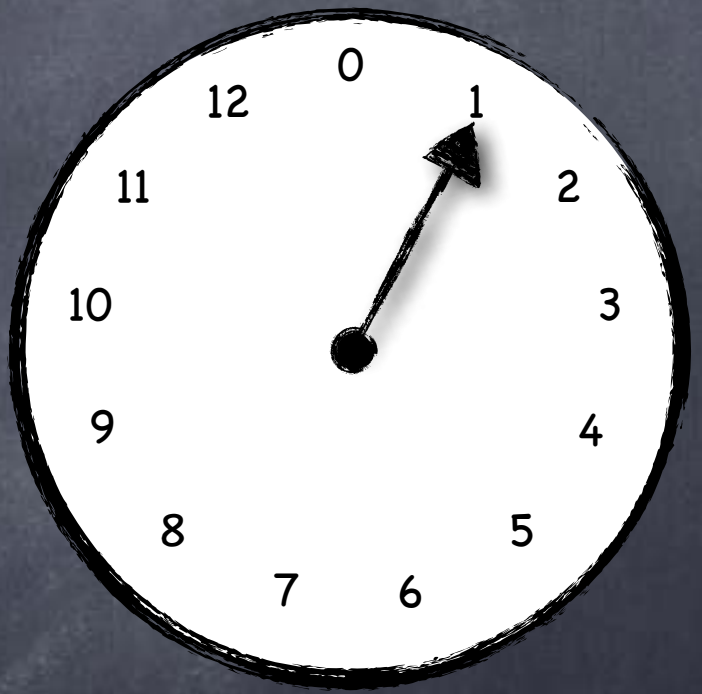
Numb3rs

Lecture 5
Modular Arithmetic



Story So Far

- Quotient and Remainder
- GCD
  - Euclid's algorithm to compute gcd(a,b)
  - $L(a,b) \triangleq \{ au + bv \mid u,v \in \mathbb{Z} \}$
    $= \{ n \cdot \gcd(a,b) \mid n \in \mathbb{Z} \}$
- Primes
  - Fundamental Theorem of Arithmetic

Question

- $2520 = 2^3 \cdot 3^2 \cdot 5 \cdot 7$
  $3300 = 2^2 \cdot 3 \cdot 5^2 \cdot 11$
  gcd (2520, 3300) =

A. 10
B. 30
C. 60
D. 150
E. 180

Common Multiples

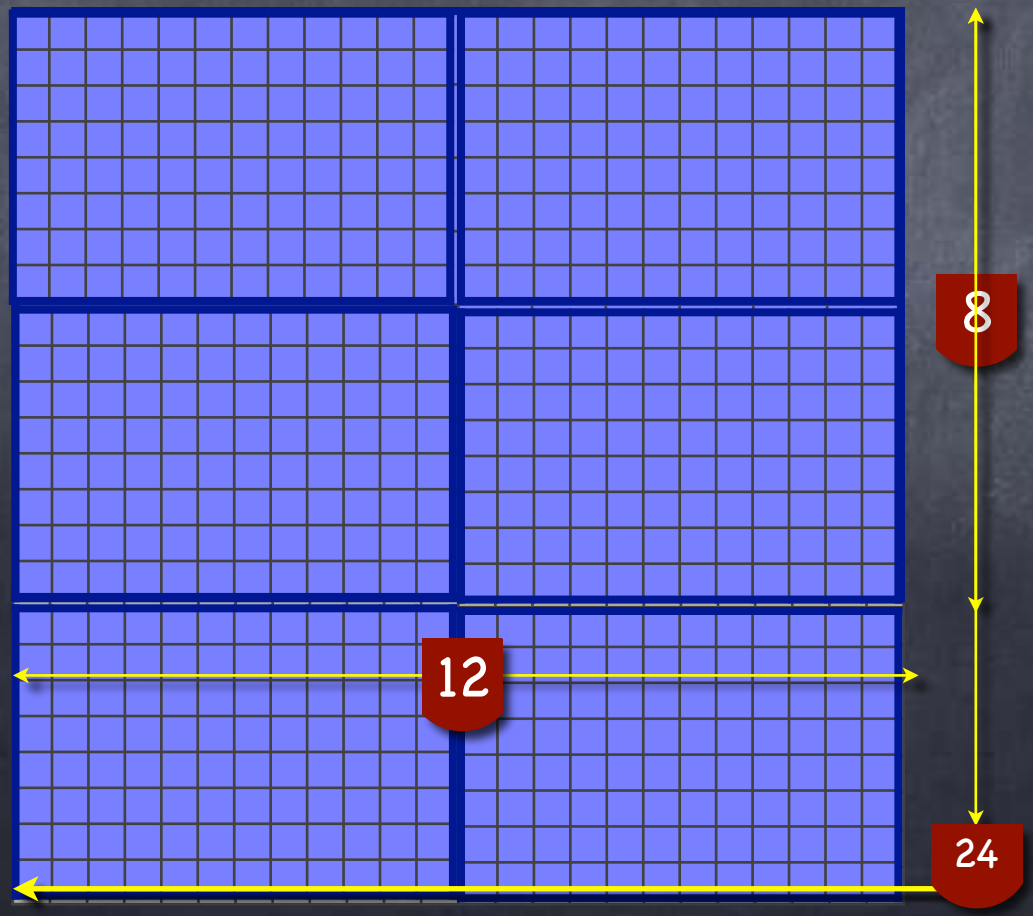
- Common Multiple: c is a common multiple of a and b if a|c and b|c.
- Least Common Multiple (for $a \neq 0$ and $b \neq 0$)
  lcm(a,b) = smallest positive integer among the common multiples of a and b
  - Well-defined: $a \cdot b$ is a positive common multiple of (a,b) (unless a=0 or b=0) and we restrict to positive multiples. So an integer in the range [1, $a \cdot b$].
  - e.g. $36 = 2^2 \cdot 3^2$, $30 = 2 \cdot 3 \cdot 5$. $\text{lcm}(36,30) = 2^2 \cdot 3^2 \cdot 5 = 180$

LCM as Tiling

[Here all numbers are positive integers]

- m is a common multiple of a & b, iff an a x b tile can be used to perfectly tile an m x m square

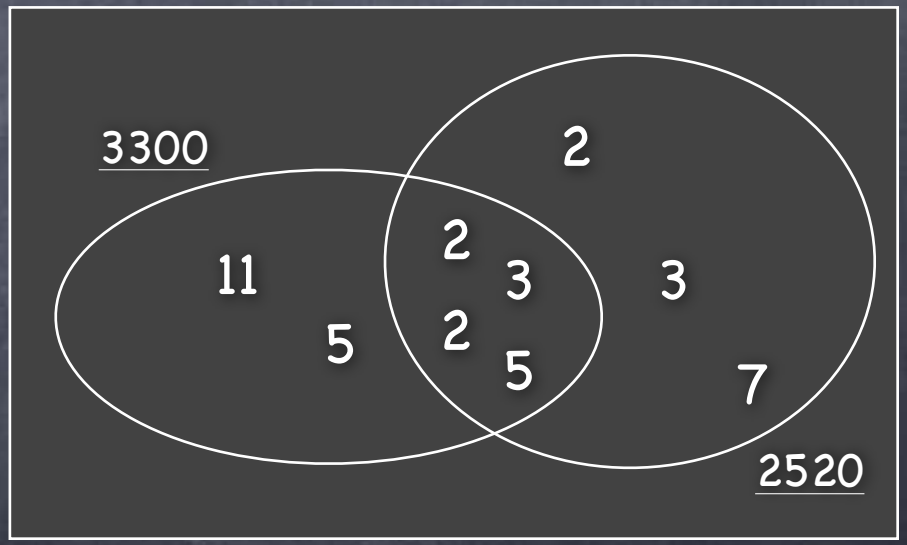
LCM: smallest such square



Question

- $2520 = 2^3 \cdot 3^2 \cdot 5 \cdot 7$
  $3300 = 2^2 \cdot 3 \cdot 5^2 \cdot 11$
  lcm (2520, 3300) =

  A. $2^5 \cdot 3^3 \cdot 5^3 \cdot 7 \cdot 11$
  B. $2^3 \cdot 3^2 \cdot 5^2 \cdot 7 \cdot 11$
  C. $2 \cdot 3 \cdot 5 \cdot 7 \cdot 11$
  D. $2^3 \cdot 3^3 \cdot 5^3 \cdot 7^3 \cdot 11^3$
  E. $2^2 \cdot 3 \cdot 5 \cdot 7 \cdot 11$

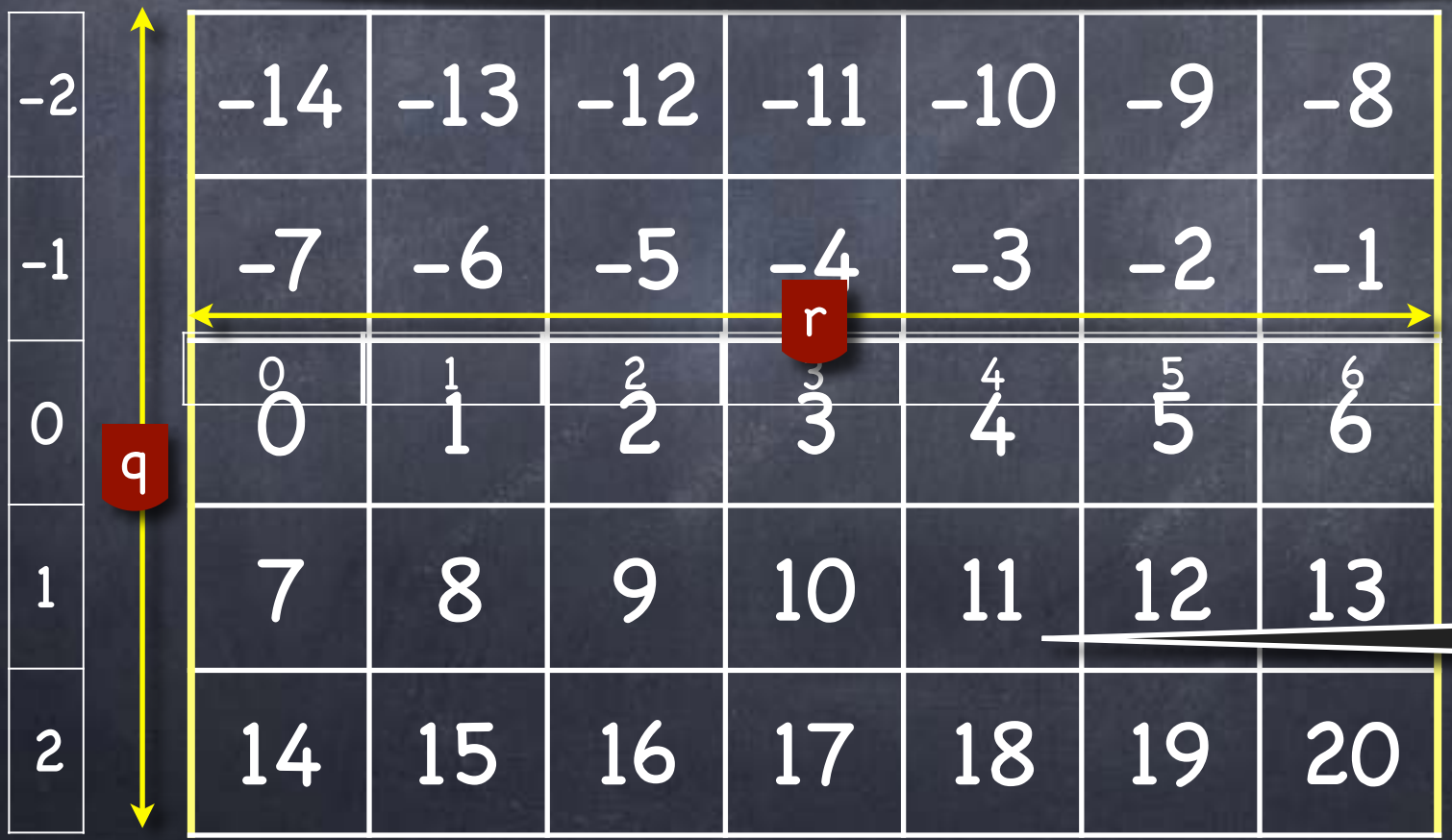


- gcd(a,b) · lcm (a,b) = |a·b| [Why?]

Quotient & Remainder

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

$$a = q \cdot m + r, \quad \text{and } 0 \le r < |m|$$



Congruence

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

- $a \equiv b \pmod{m}$ iff remainder(a,m) = remainder(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

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

modulus= 7

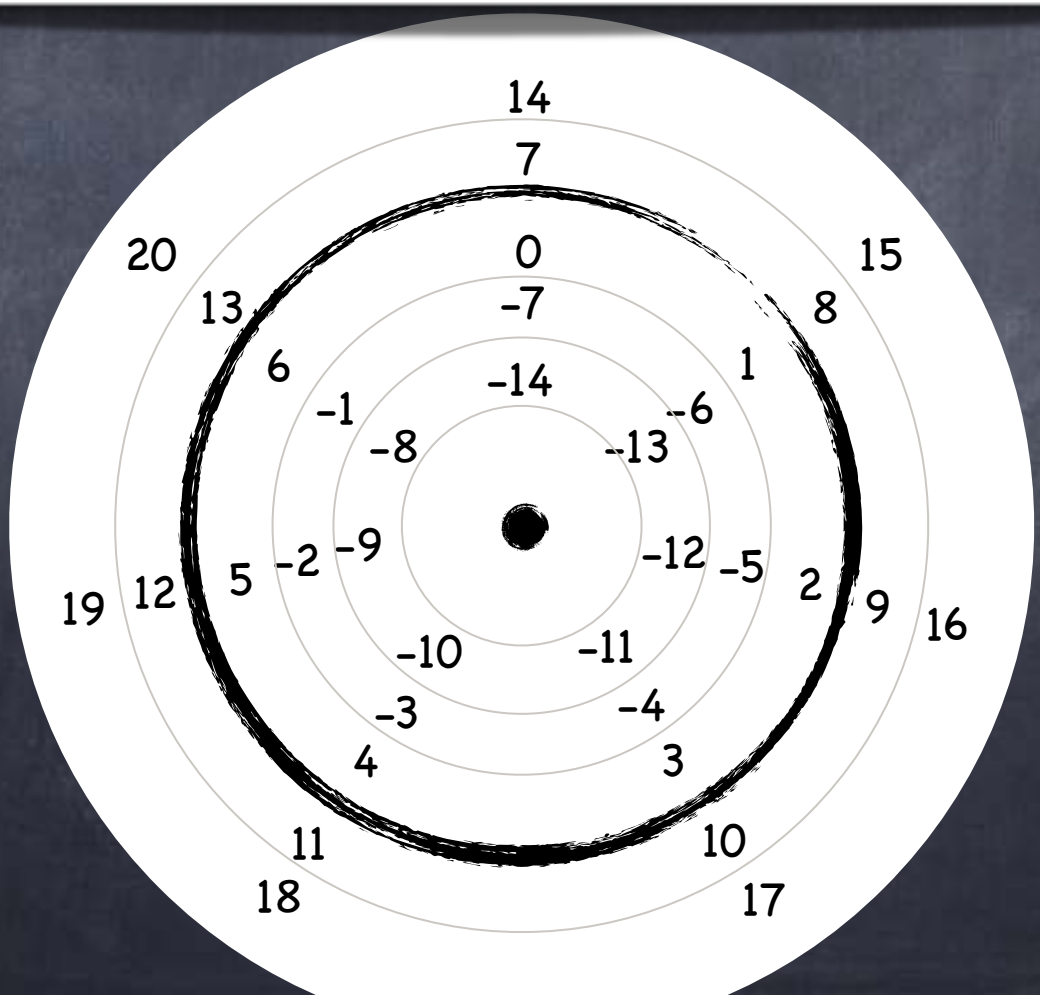
$11 \equiv 18 \pmod{7}$

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

$9 \equiv 2 \pmod{7}$

Congruence

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



modulus= 7

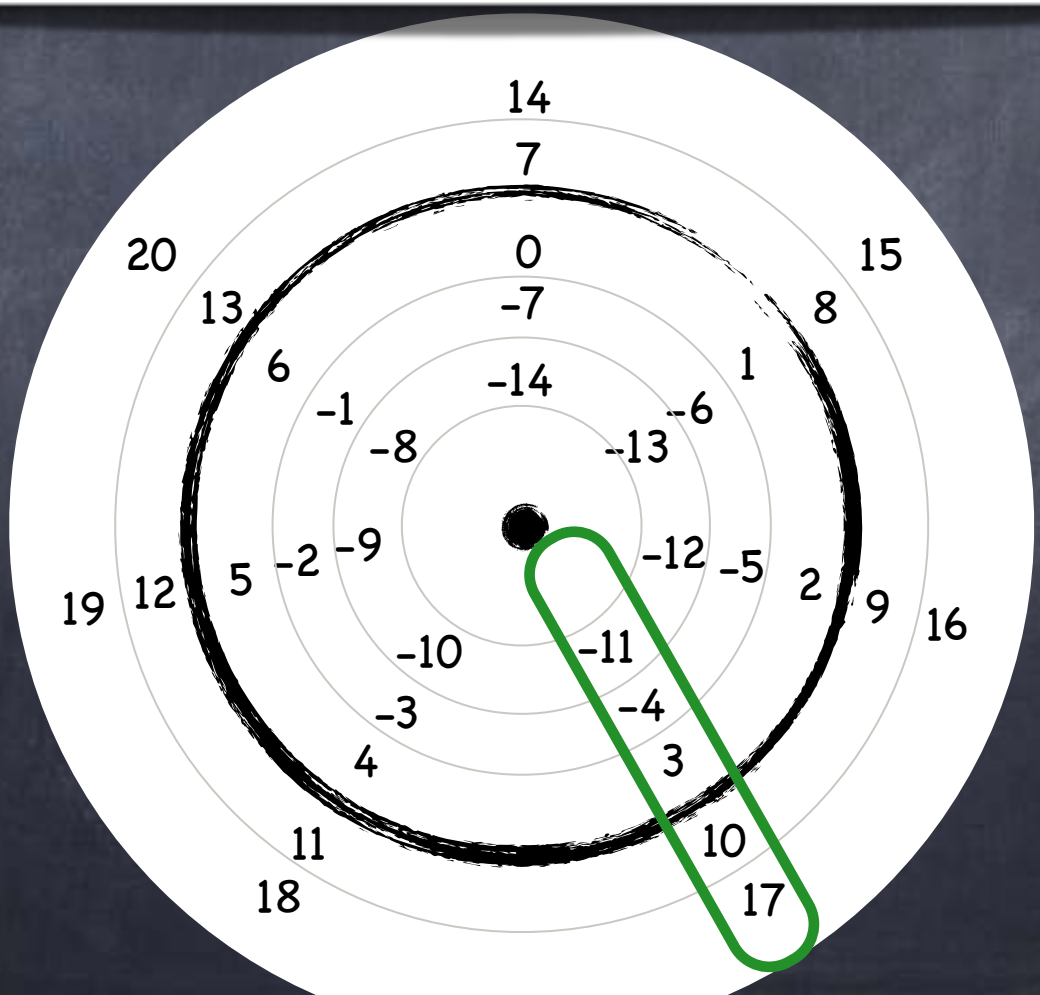
Question

- Pick correct values for x in $-11 \equiv x \pmod 7$

A. 4 and -3
B. 3 and -4
C. -3 and -4
D. 4 and -4
E. 3 and -3

Congruence

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



modulus= 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., " $\rightarrow (a+b) \equiv (a'+b') \pmod m$?
    - $(a+b)-(a'+b') = (a-a') + (b-b')$ is a multiple of m. ✔

Modular Addition

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

$1 + 4 \equiv 0 \pmod 5$
$2 + 3 \equiv 0 \pmod 5$

$7 + -25 \equiv 7 \pmod 5$

-25	-24	-23	-22	-21
-20	-19	-18	-17	-16
-15	-14	-13	-12	-11
-10	-9	-8	-7	-6
-5	-4	-3	-2	-1
0	1	2	3	4
5	6	7	8	9

$-8 + -19 \equiv 2+1 \pmod 5$

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. p = 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: $[a]_m \times_m [b]_m \triangleq [a \cdot b]_m$
  - $[a]_m = [a']_m \wedge [b]_m = [b']_m \rightarrow [a \cdot b]_m = [a' \cdot b']_m$?
    - i.e., " $\rightarrow a \cdot b \equiv a' \cdot b' \pmod m$?
    - $\exists p,p',r \quad a = pm+r,\ a'=p'm+r$
      $\exists q,q',s \quad b = qm+s,\ b'=q'm+s$ (why?)
      - $a \cdot b = (mpq+ps+qr)m + rs$ and
        $a' \cdot b' = (mp'q'+p's+q'r)m + rs$. So $m \mid (a \cdot b - a' \cdot b')$

Modular Multiplication

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

$7 \times -20 \equiv 0 \pmod 5$

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

$-8 \times -19 \equiv 2 \times 1 \pmod 5$

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. p = 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

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: $[a]_m \times_m [b]_m \triangleq [a \cdot b]_m$
- Well-defined: if $a \equiv a' \pmod m$ and $b \equiv b' \pmod m$, then
  - $a + b \equiv a' + b' \pmod m$
  - $a \cdot b \equiv a' \cdot b' \pmod m$

Question

- $8^8 \equiv x \pmod 5$ where x is

A. 0
B. 1
C. 2
D. 3
E. 4

$$8^8 \equiv 3^8 \pmod 5$$
$$3^2 \equiv 4 \pmod 5$$
$$3^4 \equiv 4^2 \equiv 1 \pmod 5$$
$$3^8 \equiv 1^2 \equiv 1 \pmod 5$$

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 p, all except $[0]_p$ have inverses!