

TEORÍA DE NÚMEROS: NÚMEROS PRIMOS

OMMGTO 2022
Jesús Liceaga
jose.liceaga@cimat.mx



¿QUÉ SON LOS NÚMEROS PRIMOS?

- Los números primos son los bloques con los que construimos a todos los enteros.
- Para esta sesión, sólo consideraremos enteros positivos.

Sean p un entero positivo. Decimos que p **es primo** si p tiene exactamente dos divisores positivos: 1 y él mismo.

- Algunos números primos son 2, 3, 5, 7, 11, etc.
- Según nuestra definición, el 1 **no** es un número primo. ¿Por qué?

NÚMEROS COMPUESTOS

Sean n un entero positivo. Decimos que n **es compuesto** si es igual al producto de dos o más primos.

- Algunos números compuestos son $4 = 2 \cdot 2$, $6 = 2 \cdot 3$, $24 = 2 \cdot 2 \cdot 2 \cdot 3$, etc.
- Según nuestra definición, el 1 **tampoco** es un número compuesto. ¿Por qué?



LA CRIBA DE ERATÓSTENES

- Es un método para encontrar números primos.

	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	29	30
31	32	33	34	35	36	37	38	39	40
41	42	43	44	45	46	47	48	49	50
51	52	53	54	55	56	57	58	59	60
61	62	63	64	65	66	67	68	69	70
71	72	73	74	75	76	77	78	79	80
81	82	83	84	85	86	87	88	89	90
91	92	93	94	95	96	97	98	99	100



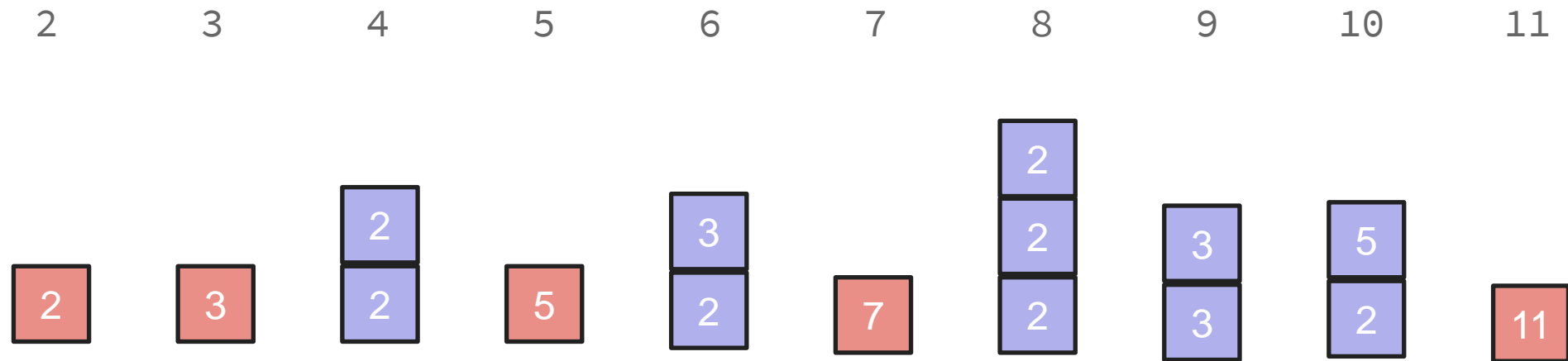
¿CÓMO SABER SI UN NÚMERO ES PRIMO?

- Dado un entero positivo n , podemos dividirlo entre todos los números menores a él. Si no es divisible entre ninguno de ellos, entonces n es primo.
- Si n es grande, lo anterior puede tomar mucho tiempo.
- Un mejor método se basa en la idea de que, si $n = a \cdot b$, entonces alguno de entre a y b debe de ser menor o igual a la raíz de n , pues si ambos fueran mayores entonces su producto sería mayor que n .
- Por lo tanto, basta revisar si n es divisible entre algún número menor o igual a su raíz.
- Por ejemplo, supongamos que queremos ver si 37 es primo.
- Como $\sqrt{37} \approx 6.08$, entonces basta ver que 37 no es divisible por ningún número entre 2 y 6, lo cuál es considerablemente menos trabajoso que ver si no es divisible por ningún número entre 2 y 36.



EL TEOREMA FUNDAMENTAL DE LA ARITMÉTICA

- Como mencionamos en un inicio, los números primos son los “bloques” con los que construimos a todos los demás enteros.



- En esta sucesión, ¿habrá infinitos bloques rojos? Es decir, ¿hay infinitos números primos?



EL TEOREMA FUNDAMENTAL DE LA ARITMÉTICA

Sea n un entero positivo distinto de 1. Entonces n es primo o se puede escribir como producto de dos o más primos. Más aún, esta forma de escribir a n es única salvo por el orden de los factores



ALGUNAS PROPIEDADES

- Los números primos también tienen algunas propiedades que nos pueden ser útiles para problemas de divisibilidad. Por ejemplo:
 1. Sean p, q dos números primos distintos y sea n un entero. Si $p|n$ y $q|n$, entonces $pq|n$.
 2. Sea p un número primo y sean a, b dos enteros. Si $p|ab$, entonces $p|a$ o $p|b$.

