Bajo que condición la siguiente afirmación es cierta?

Si $a|b\cdot c$, entonces $a|b$ o $a|c$

Por ejemplo, $6|3.4 \Rightarrow 6\nmid 3$ o $6\nmid 4$

Teorema Si $a|bc$ y $(a,b)=1$, entonces $a|c$.

Dem.

Si $a|bc \iff \boxed{bc=a\cdot t}$, $t\in\mathbb{Z}$

$(a,b)=d$

$\underline{d=ax+by}$

y $(a,b)=1 \iff 1=ax+by$ $//c$ $\exists\, x,y\in\mathbb{Z}$

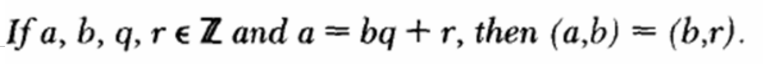
$$c=acx+\underline{bc}y$$

$$c=acx+a\cdot ty$$

$$c=a(cx+ty)$$

$$c=a\cdot r \Rightarrow a|c$$

Propiedad.



If a, b, q, r ∈ **Z** *and a* = *bq* + *r, then* (*a,b*) = (*b,r*).

Si $a,b,q,r\in\mathbb{Z}$ y $\underline{a=bq+r}$, entonces $\underbrace{(a,b)=(b,r)}$

Dem.

Sea $d=(a,b) \Rightarrow d=ax+by$ ①

$d=(b,r)$

$d=bm+rn$

Luego. $a=bq+r$ reemp. en ①

$$d=(bq+r)x+by$$

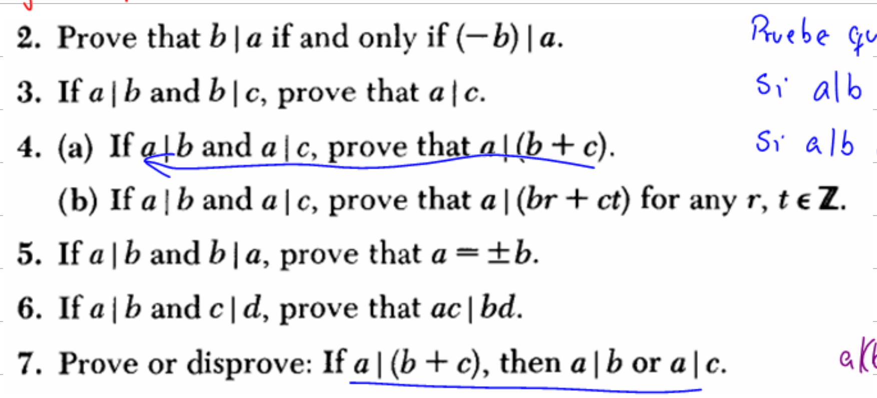
$$d=bqx+rx+by$$

$$d=b\underbrace{(qx+y)}_{m}+r\underbrace{x}_{n}$$

$$d=b\cdot m+r\cdot n$$

Así $(a,b)=(b,r)$

Ejercicios.



2. Prove that $b \mid a$ if and only if $(-b) \mid a$.

3. If $a \mid b$ and $b \mid c$, prove that $a \mid c$.

4. (a) If $a \mid b$ and $a \mid c$, prove that $a \mid (b + c)$.

(b) If $a \mid b$ and $a \mid c$, prove that $a \mid (br + ct)$ for any $r, t \in \mathbf{Z}$.

5. If $a \mid b$ and $b \mid a$, prove that $a = \pm b$.

6. If $a \mid b$ and $c \mid d$, prove that $ac \mid bd$.

7. Prove or disprove: If $a \mid (b + c)$, then $a \mid b$ or $a \mid c$.

Pruebe que $b \mid a \iff (-b) \mid a$

Si $a \mid b$ y $b \mid c \implies a \mid c$

Si $a \mid b$ y $a \mid c \implies a \mid b + c$

$a \mid (b+c) \rightarrow a \mid b \vee a \mid c$

1. Pruebe que $b \mid a \iff (-b) \mid a$ $\qquad a = (-b) \cdot K$

Dem.

Como $b \mid a \iff a = b \cdot t \quad , t \in \mathbb{Z}$

$$\iff -a = (-b) \cdot t \qquad // (-1)$$

$$\iff a = (-b)(-t) \quad , -t \in \mathbb{Z}$$

$$\iff (-b) \mid a$$

$c = a \cdot K$.

2. Si $a \mid b$ y $b \mid c \implies \boxed{a \mid c}$

Dem.

Como $a \mid b$ y $b \mid c \iff \underline{b = a \cdot t} \wedge c = b \cdot r \quad , t, r \in \mathbb{Z}$

$$\implies c = (at) \cdot r$$

$$\implies c = a(tr)$$

$$\implies c = a \cdot K$$

$$\implies a \mid c$$

3. Si $a \mid b$ y $a \mid c \implies a \mid b + c$

4. $a \mid (b+c) \rightarrow a \mid b \vee a \mid c$

Contraejemplo. $a = 5 \quad b = 9 \quad c = 1$

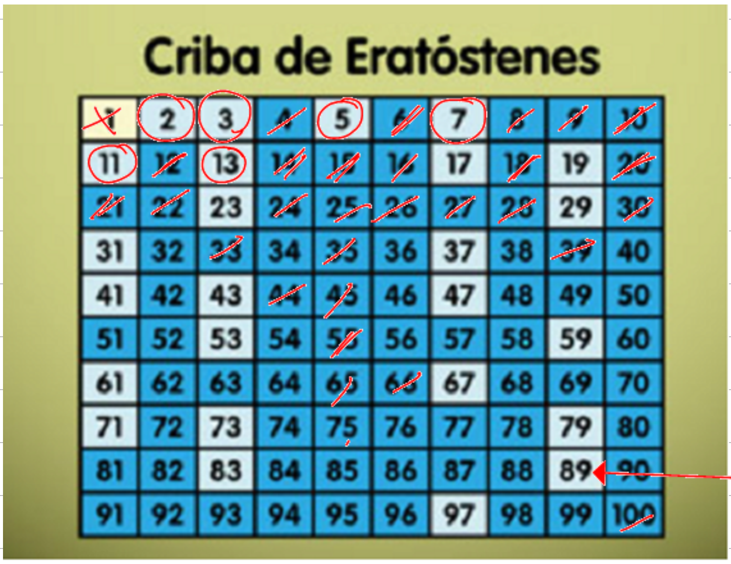
$$5 \mid 10 \rightarrow 5 \nmid 9 \vee 5 \nmid 1$$

Números y la factorización única

Def. (Número primo)

Un número p es primo si sólo es divisible entre 1 y p.

Un número que no es primo, se llama compuesto.



Criba de Eratóstenes

~~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~~	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~~

Teorema fundamental de la aritmética Todo número compuesto tiena una descomposición única en factores primos.

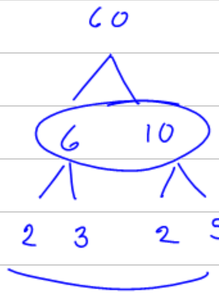
Dem.

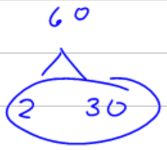
?

Ejm. Factoriza cada número.

$$60 = 2\cdot 3\cdot 2\cdot 5$$

$$= 2^2\cdot 3\cdot 5 \quad ✓$$





$$178 = 2\cdot 89$$

Teorema. El conjunto de números primos es infinito

Obs. Los primos que difieren en 2 unidades se llaman primos gemelos

Por ejm. 5 y 7 , 11 y 13 , 17 y 19 ,

Ejm. Todo primo impar es de la forma $4k+1$ o $4k-1$, $k\in\mathbb{N}$