Congruences

DEF $a \equiv b \pmod{n}$ ("congruent to", "modulo")

means $a = b + m \cdot n$ for some integer m

EG $17 \equiv 5 \pmod{12}$
$\equiv 29 \equiv -7$

EG 3/14/2020 SAT
3/14/2021 SUN

$365 \equiv 15 \equiv 1 \pmod{7}$

EG $314 + 77 \pmod{10}$
$\equiv 4 + 7 \equiv 1$

$36 \cdot 75 \pmod{11}$
$\equiv 3 \cdot 9 = 27 \equiv 5$
($9 \equiv -2$, $27 \equiv -6$)

do not compute $36 \cdot 75 = 2700$

EG Show that $41 \mid 2^{20} - 1$.

$\Leftrightarrow 2^{20} - 1 \equiv 0 \pmod{41}$

$2^5 = 32 \equiv -9 \pmod{41}$
$2^{10} = (2^5)^2 \equiv (-9)^2 = 81 \equiv -1 \pmod{41}$ ($\equiv 40$)
$2^{20} \equiv (-1)^2 = 1 \pmod{41}$

Caution: (p prime)

$ab = 0 \Rightarrow a = 0$ or $b = 0$ ($p \mid ab$; $p \mid a$, $p \mid b$)

$ab \equiv 0 \pmod{p} \Rightarrow a \equiv 0$ or $b \equiv 0 \pmod{p}$

$ab \equiv 0 \pmod{n} \not\Rightarrow a \equiv 0$ or $b \equiv 0 \pmod{n}$

EG $4 \cdot 15 \equiv 0 \pmod{6}$ ($6 = 2 \cdot 3$)
but $4 \not\equiv 0 \pmod{6}$ and $15 \not\equiv 0 \pmod{6}$