

$$a \mid bc \Rightarrow (a \mid b \text{ or } a \mid c)$$

For  $a, b, c \in \mathbb{Z}$ .

not true  
for all  $a, b, c$ .

Counter-example to this

$$a = 25$$

$$b = 10$$

$$c = 30$$

$$25 \mid \underbrace{10 \cdot 30}_{300}$$

but  $25 \nmid 10$   
and  $25 \nmid 30$

But is true when  $a$  is prime

so  $\forall b, c \in \mathbb{Z}$ . "Euclid's lemma"

$$p \mid ab \Rightarrow (p \mid a \text{ or } p \mid b)$$

---











Q8 Using modular arithmetic.

Suppose  $p, q$  are primes  $p, q \geq 5$

Claim  $p^2 - q^2$  is divisible 24.

i.e. we will show  $8 \mid p^2 - q^2$

and that  $3 \mid p^2 - q^2$

(gcd(a,b)=1 then  $(a \mid c \& b \mid c) \Rightarrow ab \mid c$ )

Think modulo 3

$$p \equiv 1, 2 \pmod{3}, q \equiv 1, 2 \pmod{3}$$

$$\Rightarrow p^2 \equiv 1 \pmod{3}, q^2 \equiv 1 \pmod{3}$$

$$\Rightarrow p^2 - q^2 \equiv 0 \pmod{3}$$

$$\Rightarrow 3 \mid p^2 - q^2 \quad \checkmark$$



$$2012^{2012} \equiv (2012^2)^{1006} \pmod{5}.$$

$$\equiv 2^{2012} \pmod{5}$$

since  $2012 \equiv 2 \pmod{5}$

$\boxed{\pmod{5}}$

0

$$2^2 \equiv 4$$

$$2^3 \equiv 3$$

$$2 \equiv 2^1$$

$$\begin{array}{c} 2^4 \\ ||| \\ 2^0 \\ ||| \\ 1 \end{array}$$

and  $2012 \equiv 0 \pmod{4}$

so  $2^{2012} \equiv (2^4)^{503} \pmod{5}$



