spoiler: primes are special

$\Rightarrow$ sketched

$\Leftarrow$

$$\forall n \in \mathbb{N}, (n > 1 \land (\forall a, b \in \mathbb{N}, n \nmid a \land n \nmid b \Rightarrow n \nmid ab)) \Leftrightarrow Prime(n)$$

discuss $\quad \gcd(n, a) = 1 = \gcd(n, b)$

means $\quad$ we have $s_1 n + t_2 a = 1 = s_2 n + t_2 b$

... $\quad s_3 n + t_3 ab = 1$ ... $\gcd(n, ab) = 1$

... $n \nmid ab$

spoiler: primes are special

$$\forall n \in \mathbb{N}, (\underbrace{n > 1}_{\text{Part I}} \wedge \underbrace{(\forall a, b \in \mathbb{N}, n \nmid a \wedge n \nmid b \Rightarrow n \nmid ab)}_{\text{Part II}}) \Leftrightarrow \underline{Prime(n)}$$

Proof

Let $n \in \mathbb{N}$. assume $Prime(n)$.

For part I, definition of $Prime(n)$ say "$n > 1 \wedge \dots$". So, $n > 1$.

For part II, let $a, b \in \mathbb{N}$. assume $n \nmid a \wedge n \nmid b$. So, $gcd(n,a) = 1 = gcd(n,b)$, since n's only divisors are 1 and n. By claim 6 ($\leftarrow$) this means $\exists s_1, s_2, t_1, t_2 \in \mathbb{Z}$, $s_1 a + t_1 n = 1 = s_2 b + t_2 n$.

Let s_1, s_2, t_1, t_2 be such values.

Let $s_3 = \underline{s_1 s_2}$, let $t_3 = \underline{s_1 t_2 a + s_2 t_1 b + t_1 t_2 n}$.

Want to show $s_3 ab + t_3 n = 1$.

spoiler: primes are special

$$\forall n \in \mathbb{N}, (n > 1 \wedge (\forall a, b \in \mathbb{N}, n \nmid a \wedge n \nmid b \Rightarrow n \nmid ab)) \Leftrightarrow Prime(n)$$

~~Then $(s_1 a + t_1 b)(s_2 b + t_2 \ ) = s_1 s_2 ab$~~ $+ \quad \overset{a}{\downarrow} \quad \overset{b}{\downarrow}$

Then $(s_1 a + t_1 n)(s_2 b + t_2 n) = s_1 s_2 ab + (s_1 t_2 + s_2 t_1 + t_1 t_2 n) n$

$= s_3 ab + t_3 n$

By Claim 5, we know $\gcd(ab, n) \mid 1. \wedge \gcd(ab,n) \geq 1$

So $\gcd(ab,n) = 1$. So $n \nmid ab$.

prove converse...

$$\forall n \in \mathbb{N}, (n > 1 \wedge (\forall a, b \in \mathbb{N}, n \nmid a \wedge n \nmid b \Rightarrow n \nmid ab)) \Leftrightarrow Prime(n)$$

linear combinations

$\forall a, b, c, p, q \in \mathbb{Z}, (a \quad b \wedge a \quad c \Rightarrow a \quad (bp + cq))$

discuss

$a \mid b \Rightarrow \exists k_1 \in \mathbb{Z}, \; b = k_1 a$

$a \mid c \Rightarrow \exists k_2 \in \mathbb{Z}, \; c = k_2 a$

$\forall p, q \in \mathbb{Z} \quad pb + qc = p k_1 a + q k_2 a$

modular multiplication $n \mid (a-c) \wedge n \mid (b-d)$

$\forall a, b, c, d, n \in \mathbb{Z}, n \neq 0 \wedge a \equiv c \pmod{n} \wedge b \equiv d \pmod{m} \Rightarrow ab \equiv cd \pmod{n}$

<u>discuss</u>

$n \mid (a-c)$ want $n \mid (ab-cd)$

$n \mid (b-d)$

try $n \mid b(a-c) + c(b-d)$

or $n \mid (ba-cd)$

Notes

eg $8 \equiv 1 \pmod{7}$

$$8^2 \equiv 1^2 \pmod{7}$$

$$8^4 \equiv (1^2)^2 \pmod{7}$$

$$9^{1000} \overset{?}{\equiv} \qquad \pmod{7}$$

$$9 \equiv 2 \pmod{7}$$

$$9^2 \equiv 4 \pmod{7}$$

$$9^3 \equiv 1 \pmod{7}$$

$$9^{1000} \equiv (9^3)^{333} \cdot 9 \pmod{7}$$

$$\equiv (1)^{333} \cdot 2 \pmod{7}$$