

Problem: Prove :

$$\forall a, b \in \mathbb{Z}^+, 49|(a^2 + b^2) \Rightarrow 7|a \wedge 7|b$$

Proof: I will prove an equivalent statement which is the contrapositive:

$$\forall a, b \in \mathbb{Z}^+, 7 \nmid a \vee 7 \nmid b \Rightarrow 49 \nmid (a^2 + b^2)$$

I will discuss the cases: $7 \nmid a \vee 7 \nmid b \equiv \underbrace{[(7|a \wedge 7 \nmid b) \oplus (7 \nmid a \wedge 7|b)]}_{\text{case 1,2}} \oplus \underbrace{(7 \nmid a \wedge 7 \nmid b)}_{\text{case 3}}$ ¹

Case 1,2: Suppose without loss of generality that $7|a \wedge 7 \nmid b$, then $49 \nmid (a^2 + b^2)$ holds always. Because if not, then we must have $7|b$ and this contradicts with $7 \nmid b$.

Case 3: This the core of the proof. Suppose $7 \nmid a \wedge 7 \nmid b$, then we can write

$$a = 7n_1 + r_1, b = 7n_2 + r_2 \quad : \quad 1 \leq r_1, r_2 \leq 6$$

Then:

$$a^2 + b^2 = \underbrace{49(n_1^2 + n_2^2) + 14(n_1r_1 + n_2r_2)}_{\text{divisible by 7}} + (r_1^2 + r_2^2)$$

Therefore, $7|a^2 + b^2$ iff $\exists r_1, r_2$ such that $7|r_1^2 + r_2^2$ and $1 \leq r_1, r_2 \leq 6$. Since r_1, r_2 have finite set of possible values, then all this values can be tried. By trying them all (tedious to list), we find that no such r_1, r_2 exists. Therefore, $7 \nmid (a^2 + b^2)$ which implies $49 \nmid (a^2 + b^2)$. QED

¹ \oplus denotes exclusive OR