Prove he has x, s.t. $\boxed{x^2+4x+7=0}$, mod 997 (p), without showing x while hiding x

Requirements: ① A separate verification setup ② Challenges
③ Acceptance criteria

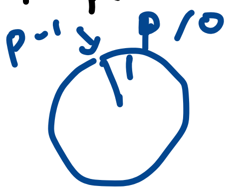
① Setup. $V(I) = 300^{I}$

② Challenge. Ask prover to send A $(=300^{x^2})$ and B $(=300^{4x})$

③ Acceptance Criteria. Verifies that $A \cdot B \cdot 300^{6} = 1$. If so, accept!

Consider $\underline{V(I) = 300^I}$, 300 is a generator for prime field with $p=997$

Properties ① g, $g^{p-1} = 1$ ② If $I = p-1 \pmod{997}$, then $V(I)$ or $300^{p-1} = 1$



p-1

Idea: Let $I = (x^2+4x+7)-1$, then $V(I) = \boxed{300^{x^2+4x+6} = 1}$

mod 997

Alternative Statement (equivalent)

Why? Simplify: $\boxed{300^{x^2 \bmod 997} \cdot 300^{4x \bmod 997} \cdot 300^{6} = 1}$

A

B

$\boxed{300^{x^2}} = \underbrace{300 \cdot 300 \cdots 300}_{x^2 \text{ times}}$

$\boxed{300^{4x}} = \underbrace{300 \cdot 300 \cdot 300 \cdots 300}_{4x \text{ times}}$