

Case 2: $p \mid a^2 + a + 1$

$$\Rightarrow a-1 \mid p-1 \Rightarrow p > a-1 \Rightarrow \gcd(p, a-1) = 1$$

$$m = \frac{a^2 + a + 1}{p} \in \mathbb{Z}$$

$$\begin{cases} a^2 + a + 1 \equiv 3 \pmod{a-1} \\ p \equiv 1 \pmod{a-1} \end{cases} \Rightarrow a^2 + a + 1 \equiv 3p \pmod{a-1}$$

$$\Rightarrow mp \equiv 3p \pmod{a-1} \\ m \equiv 3 \pmod{a-1}$$

since $\gcd(p, a-1) = 1$

$$\Rightarrow m = 3 \quad \text{or} \quad m \geq (a-1) + 3$$

• if $m = 3$:

$$\begin{cases} a^2 + a + 1 = 3p \\ p-1 = 3(a-1) \end{cases} \Rightarrow a^2 + a + 1 = 9a - 6$$

$$\Rightarrow a^2 - 8a + 7 = 0$$

$$\Rightarrow (a-7)(a-1) = 0$$

$$\Rightarrow \boxed{a=7, p=19} \mid \begin{matrix} a=1 \\ p=0 \end{matrix} \times$$

• if $m \geq a+2$

$$\Rightarrow a^2 + a + 1 \geq (a+2)p$$

$$\Rightarrow \frac{a^2 + a + 1}{a+2} \geq p \Rightarrow a > p$$

$$\Rightarrow a-1 > p-1$$

$$\text{but } a-1 \mid p-1 \Rightarrow \Leftarrow !!$$