Proof. From definition, $S_p = \{n : x^n - 1 \equiv (x^p - x + 1)f(x) \mod p \quad \text{for some } f(x)\}$.

Claim. $2\frac{p^p-1}{p-1} = 2(p^{p-1} + \cdots + 1)$, $p^p - 1 = (p-1)(p^{p-1} + \cdots + 1) \in S_p$

Proof. Let α be any root of $x^p - x + 1 = 0$ over $\mathbb{F}_p$. Observe that $\alpha^p = \alpha - 1$. Then $(\alpha+1)^p - (\alpha+1) + 1 = \alpha^p + 1^p - \alpha = (\alpha - 1) + 1 - \alpha = 0$, which means that $\alpha + 1$ is also a root of the polynomial $x^p - x + 1$. Similarly, $\alpha + a$ is a root for any $a \in \mathbb{F}_p$. Because the polynomial has p roots and $\alpha + a$'s are pairwise distinct for $a \in \mathbb{F}_p$, we get

$$x^p - x + 1 \equiv \prod_{a=0}^{p-1}(x - \alpha - a) \mod p$$

Let $m = p^{p-1} + \cdots + 1$. To show the claim, it is enough to show that $x^{2m} - 1$ and $x^{(p-1)m} - 1$ are divided by $x^p - x + 1$ over $\mathbb{F}_p$, in other words, any root α of $x^p - x + 1$, $\alpha^{2m} = \alpha^{(p-1)m} = 1$ over $\mathbb{F}_p$.
From the factorization of $x^p - x + 1$, we can observe that $\prod_{a=0}^{p-1}(-\alpha - a) = 1$. Also, since $\alpha^p = \alpha - 1$,

$$\alpha^{p^k} = (\alpha^p)^{p^{k-1}} = (\alpha - 1)^{p^{k-1}} = \alpha^{p^{k-1}} + (-1)^p = \cdots = \alpha^{p^0} + k \times (-1)^p = \alpha + k(-1)^p$$

for every $k \in \mathbb{N}$. Using these equalities, we get

$$\begin{aligned}
\alpha^{2m} &= \left(\alpha^{\sum_{k=0}^{p-1} p^k}\right)^2 = \left(\prod_{k=0}^{p-1} \alpha^{p^k}\right)^2 \\
&= \prod_{k=0}^{p-1}(\alpha + k(-1)^p)^2 = \prod_{k=0}^{p-1}(\alpha + k)^2 = \prod_{k=0}^{p-1}(-\alpha - k)^2 = \left(\prod_{k=0}^{p-1}(-\alpha - k)\right)^2 = 1 \\
\alpha^{(p-1)m} &= \left(\alpha^{\sum_{k=0}^{p-1} p^k}\right)^{p-1} = \left(\prod_{k=0}^{p-1} \alpha^{p^k}\right)^{p-1} \\
&= \left(\prod_{k=0}^{p-1}(\alpha + k(-1)^p)\right)^{p-1} = \left(\prod_{k=0}^{p-1}(\alpha + k)\right)^{p-1} \\
&= \left((-1)^p \prod_{k=0}^{p-1}(-\alpha - k)\right)^{p-1} = (-1)^{p(p-1)} = 1
\end{aligned}$$

over $\mathbb{F}_p$, which proves the claim. $\square$

When $p > 3$, $2\frac{p^p-1}{p-1} < p^p - 1$. Thus $p^p - 1$ is not a minimum of S_p for $p > 3$. We want to prove that $p^p - 1$ is the minimum of S_p when $p = 2, 3$. Suppose that $m = \min S_p$. Note that when $s, t \in S_p$, $x^s - 1$ and $x^t - 1 (s > t)$ are both divided by $x^p - x + 1$ over $\mathbb{F}_p$, $x^s - x^t = x^t(x^{s-t} - 1)$ is divided, thus $x^{s-t} - 1$ is divided by $x^p - x + 1$. Then by using division algorithm, $x^{\gcd(s,t)} - 1$ is divided by $x^p - x + 1$ over $\mathbb{F}_p$, so $\gcd(s, t) \in S_p$. Therefore since $\gcd(m, p^p - 1) \in S_p$ and $\gcd(m, p^p - 1) \leq m$, m is a divisor of $p^p - 1$. From the fact that $x^p - x + 1$ divides $x^m - 1$, $p \leq m$.
When $p = 2$, $p^p - 1 = 3$. Since m divides 3 and $m \geq 2$, $m = 3 = p^p - 1$.

When $p = 3$, $p^p - 1 = 26$. Since m divides 26 and $m \geq 3$, $m = 13$ or 26. Since $x^{13} + 1 = (x^3 - x + 1)(x^{10} + x^8 - x^7 + x^6 + x^5 - x^4 + x^2 + x + 1)$ over $\mathbb{F}_3$ and $x^{13} + 1 - (x^{13} - 1) \not\equiv 0 \mod 3$, $m \neq 13$. Thus $m = 26 = p^p - 1$.
Therefore, primes p for which $p^p - 1$ is the minimum of S_p are 2 and 3. $\square$