If we compute $\gcd(S_{n+2}, S_{n+1})$ using Euclidean algo, the first step is to divide S_{n+2} by S_{n+1}.

(A) $$S_{n+2} = q\, S_{n+1} + r$$

where $0 \leq r < S_{n+1}$. On the other hand, by definition of S_{n+2}, we have

(B) $$S_{n+2} = 2 \cdot S_{n+1} + S_n.$$

If we show that $0 \leq S_n < S_{n+1}$, then the uniqueness part of the division algorithm tells us that

$$q = 2 \qquad r = S_n.$$

$\longrightarrow$ Next step: divide S_{n+1} by S_n. That's the first step of computing $\gcd(S_{n+1}, S_n)$

$$\overset{2}{\underset{\shortparallel}{S_2}} > \overset{1}{\underset{\shortparallel}{S_1}} \geq 0$$

$\rightarrow$ $S_{n+1} = 2 \cdot S_n + S_{n-1} > S_n \geq 0$

$$a = a_d 2^d + a_{d-1} 2^{d-1} + \cdots + a_1 2 + a_0 \qquad a_0, \ldots, a_d = 0 \text{ or } 1.$$

$$= \sum_{\text{even } k} a_k 2^k + \sum_{\text{odd } k} a_k 2^k$$

$2^k \equiv 1$ if k even
$\equiv -1$ if k odd

$$\equiv \sum_{\text{even } k} a_k + \sum_{\text{odd } k} (-a_k)$$

$$= \sum_{\text{even } k} a_k - \sum_{\text{odd } k} a_k.$$

Notice that $\sum_{\text{even } k} a_k = \#$ of 1's in even positions $= m$.

$\sum_{\text{odd}} a_k = \#$ of 1's in odd positions $= n$

$\rightsquigarrow$ $a \equiv m - n \pmod 3$.

① $a^{\varphi(p^n)} = 1 + q_n p^n$ for some q_n which is not div. by p.

<u>$n=1$.</u> $a^{\varphi(p)} = 1 + q_1 p$ for some q_1 that's not div. by p.

$a^{\varphi(p)} = a^{p-1} \equiv 1 \pmod p$ so $a^{\varphi(p)} - 1 = q_1 p$ for some q_1.
want to show that q_1 is not divisible by p.
Suppose $p \mid q_1$. Then $a^{\varphi(p)} \equiv 1 \pmod{p^2}$, but a is a primitive root of p^2 so $\varphi(p^2)$ should be the smallest power of a which is congruent to 1 mod p^2, and $\varphi(p) < \varphi(p^2)$.
Contradiction!

<u>Inductive step</u> Assume that $a^{\varphi(p^n)} = 1 + q_n p^n$ for some q_n not div. by p.
want to show that $a^{\varphi(p^{n+1})} = 1 + q_{n+1} p^{n+1}$ for some q_{n+1} not div. by p.

② Let d_n be order of a mod p^n.
want to show that $d_n = \varphi(p^n)$. for all $n \geq 2$.

<u>$n=2$</u> Immediate since a primitive root of p^2.

<u>Inductive step</u>. Assume that $d_k = \varphi(p^k)$, and we want to show that $d_{k+1} = \varphi(p^{k+1})$.

thm 8.1

(a) Explain why $\varphi(p^k) \mid d_{k+1}$ & $d_{k+1} \mid \varphi(p^{k+1})$.

$a^{d_{k+1}} \equiv 1 \pmod{p^{k+1}}$
$a^{d_{k+1}} \equiv 1 \pmod{p^k}$

a has order $\varphi(p^k)$ mod p^k,
so thm 8.1, $\varphi(p^k) \mid d_{k+1}$.

$\varphi(p^k) = p^{k-1}(p-1)$ & $\varphi(p^{k+1}) = p^k(p-1)$
so knowing that $\varphi(p^k) \mid d_{k+1} \mid \varphi(p^{k+1})$ means that $d_{k+1} = p^{k-1}(p-1)$ or $p^k(p-1)$.

(b). Assume $d_{k+1} = \varphi(p^k)$ and use ① to derive a contradiction.

$$a^{\varphi(p^k)} = a^{d_{k+1}} \equiv 1 \pmod{p^{k+1}}$$

so $a^{\varphi(p^k)} = 1 + q p^{k+1}$ for some q.
$= 1 + (qp)p^k$

so $q_k = qp$ is div by p, which is a contradiction.

$m^4 \equiv -1 \pmod p \quad (*)$

$m^8 = (m^4)^2 \equiv 1 \pmod p$

Thm 8.1 tells us that, if k is order of m mod p, then $k \mid 8$.

So $k = 1, 2, 4,$ or 8.

But, if $k = 1, 2,$ or 4, then $m^k \equiv 1 \pmod p \Rightarrow m^4 \equiv 1 \pmod p$ contradicts $(*)$.

$8.1 \Rightarrow 8 \mid \varphi(p) = p-1$

$p_1, \dots, p_r$

$n = (2p_1 \cdots p_r)^4 + 1$

Let p be a prime divisor of n. p must be odd, since n is odd.

By part (a), $p \equiv 1 \pmod 8$, so p is one of the primes $p_1, \dots, p_r$.

So $p \mid p_1 \cdots p_r \Rightarrow p \mid (2p_1 \cdots p_r)^4$. But $p \mid n$ also, so $p \mid 1$. ※.

$t_1 + \cdots + t_n = \frac{n(n+1)(n+2)}{6}$ $\qquad \frac{t_1 + \cdots + t_n}{n} = \frac{(n+1)(n+2)}{6}$ should be an integer.

n	$\frac{(n+1)(n+2)}{6}$
1	$\frac{2\cdot3}{6} = 1$
2	$\frac{3\cdot4}{6} = 2$
3	$\frac{4\cdot5}{6} \notin \mathbb{Z}$.
4	$\frac{5\cdot6}{6} = 5$
5	$\frac{6\cdot7}{6} = 7$
6	$\frac{7\cdot8}{6} \notin \mathbb{Z}$.
7	$\frac{8\cdot9}{6} = 12$
8	$\frac{9\cdot10}{6} = 15$

9 $\frac{10 \cdot 11}{6} \notin \mathbb{Z}$

$$\{n \mid n \mid (t_1 + \cdots + t_n)\} = \{n \mid 3 \nmid n\}$$

$n = 4k+1$

want to use that to show that

$$a^n \equiv a \pmod{10}.$$

We can do this by breaking up into 2 congruences:

$$a^n \equiv a \pmod 2$$
$$a^n \equiv a \pmod 5.$$

$a^n \equiv a \pmod 2$ is clear even w/out Fermat's thm. (It doesn't matter that $n = 4k+1$).

Mod 5: case 1: if $5 \mid a$, then $5 \mid a^n$ so $a^n \equiv 0 \equiv a \pmod 5$.

case 2: if $5 \nmid a$, then $a^4 \equiv 1 \pmod 5$ by Fermat's thm, so

$$a^n = a^{4k+1} = (a^4)^k \cdot a \equiv a \pmod 5.$$

$$S = \{n \in \mathbb{N} \mid n \equiv 1 \pmod 4\}.$$

① $\{n \in \mathbb{N} \mid n \equiv 1 \pmod 4\} \subseteq S$

To show this, we assume that $n \equiv 1 \pmod 4$, ie, $n = 4k+1$ for some k, and we prove that $a^n \equiv a \pmod{10}$.

② $S \subseteq \{n \in \mathbb{N} \mid n \equiv 1 \pmod 4\}$

To show this, we assume that n has the property that $a^n \equiv a \pmod{10}$ for all a.

We want to use this to show that $n \equiv 1 \pmod 4$.

$a = 3$. I know that $3^n \equiv 3 \pmod{10}$. But $\gcd(10, 3) = 1$, so

$$3^{n-1} \equiv 1 \pmod{10}.$$

Calculate & check that 3 has order 4 mod 10.

$$\left[\begin{array}{l} 3^2 = \\ 3^3 = \\ 3^4 \equiv 1 \end{array}\right)$$

so by thm 8.1, $4 \mid n-1$.