S.R-S, Chapter 4, problem 1(d)

find $0 < m < 101$ such that $m \equiv 5^{93} \pmod{101}$

Ingredients: 1. Fermat's Little Theorem (FLT) [for p prime, $0<a<p$, $a^{p-1} \equiv 1 \pmod{p}$]

2. Bezout's identity [for $a,b \in \mathbb{Z}$, $\gcd(a,b) = m \cdot a + n \cdot b$ for some ~~a, b~~ $m,n \in \mathbb{Z}$]

3. The Euclidean algorithm for calculating $\gcd(a,b)$ [S.R-S 4.3]

First, notice that 101 is prime. We only need ~~the~~ to check primes up to $\sqrt{101} \approx 10$: 2,3,5,7. 101 is not even, its digits do not add to 3,6,or 9, and doesn't end in a "5", so really you only need to check 7. You can verify that $7 \nmid 101$ ("does not divide"). Therefore FLT applies, so we know that $5^{100} \equiv 1 \pmod{101}$.

Rewrite this equivalence as $5^{93} \cdot 5^{7} \equiv 1 \pmod{101}$. Since we are working in "$\mathbb{Z}/101\mathbb{Z}$" (see def'n 4.8), we can replace 5^{93} with m, which is the quantity we are looking for. Thus, we now have the equation $m \cdot 5^{7} \equiv 1 \pmod{101}$.

You can calcutate $5^7 \pmod{101}$ and find $52 \equiv 5^7 \pmod{101}$, so our FLT identity becomes $m \cdot 52 \equiv 1 \pmod{101}$

Recall that if I see the equivalence $a \equiv b \pmod{c}$, this means that for some integer n, we have the relationship $a - n \cdot c = b$, and you may think of this n as the integer solution to a/c and b as the remainder. Realizing this, we rewrite the FLT identity again as $m \cdot 52 - n \cdot 101 = 1$, where we are looking for m such that $0 < m < 101$.

Our FLT identity looks a lot like Bezout's identity now! If $\gcd(101,52) = 1$, then we can use the Euclidean algorithm to solve for m.

S.R-S Chapter 4, problem 1 (d), continued

Apply the Euclean algorithm to gcd(101, 52):

(a) $101 \div 52 = 1 \;R\; 49 \iff 101-52=\boxed{49}$
(b) $52 \div 49 = 1 \;R\; 3 \iff 52-49=\boxed{3}$
(c) $49 \div 3 = 16 \;R\; 1 \iff 49-16\cdot\boxed{3}=1$
(d) $3 \div 1 = 3 \;R\; 0 \Rightarrow \gcd(101,52)=1$

We want to solve for m, n where $m\cdot 52 - n\cdot 101 = 1$, and equation (c) gives us a ~~fed~~ relationship for 1 in terms of 49 and 3. If we substitute (a) into (b), and then (b), and (a) into (c), we get a solution to our problem.

(a)→(b): $52-(\underbrace{101-52}_{49})=3 \Rightarrow 2\cdot 52-101=3$

(a),(b)→(c): $(\underbrace{101-52}_{49})-16(\underbrace{2\cdot 52-101}_{3})=1$

$$101-52-32\cdot 52+16\cdot 101=1$$
$$(17)(101)-(33)(52)=1$$

We are close, but we have now $m=-33$ and $n=-17$. The number between 0 and 101 congruent to -33 is $-33+101=68$, so the solution to $m=5^{93} \pmod{101}$ is $\boxed{m=68}$

Notice that for any $n\in\mathbb{Z}$, $n\cdot(101)+68(52)\equiv 1 \pmod{101}$ because $101\equiv 0 \pmod{101}$.

Bonus: for part (a) of problem 1, SR-S asks for $10^3 \pmod 7$. A quick way to solve this is to use $10\equiv 3 \pmod 7$, so

$$10^3\equiv 3^3=(\underbrace{3\cdot 3}_{2})\cdot 3 \pmod 7$$
$$=2\cdot 3=6 \pmod 7$$, which is the same as what you got.