Problem 1

Show that 91 is a pseudoprime to bases 3 and 17.

We need to show that $3^{91} \equiv 3 \pmod{91}$ and $17^{91} \equiv 17 \pmod{91}$. Since $(3, 91) = (17, 91) = 1$, we can use Euler's method. We need to find $\phi(91)$ first.

$$\begin{aligned} 91 &= 7 \times 13 \\ \phi(91) &= 91\left(1 - \frac{1}{7}\right)\left(1 - \frac{1}{13}\right) \\ &= 91\left(\frac{6}{7}\right)\left(\frac{12}{13}\right) \\ &= 72 \end{aligned}$$

Thus, $3^{72} \equiv 1 \pmod{91}$ and $17^{72} \equiv 1 \pmod{91}$. Let's make a squaring table for 3.

$$\begin{aligned} 3^1 &\equiv 3 \pmod{91} \\ 3^2 &\equiv 9 \pmod{91} \\ 3^4 &\equiv 81 \pmod{91} \\ 3^8 &\equiv 6561 \equiv 9 \pmod{91} \\ 3^{16} &\equiv 81 \pmod{91} \end{aligned}$$

$$\begin{aligned} 3^{91} &\equiv 3^{72+16+2+1} \pmod{91} \\ &\equiv 3^{72} \cdot 3^{16} \cdot 3^2 \cdot 3^1 \pmod{91} \\ &\equiv 1 \cdot 81 \cdot 9 \cdot 3 \pmod{91} \\ &\equiv 2187 \pmod{91} \\ &\equiv 3 \pmod{91} \end{aligned}$$

Now, let's make a squaring table for 17.

$$\begin{aligned} 17^1 &\equiv 17 \pmod{91} \\ 17^2 &\equiv 289 \equiv 16 \pmod{91} \\ 17^4 &\equiv 256 \equiv 74 \pmod{91} \\ 17^8 &\equiv 5476 \equiv 16 \pmod{91} \\ 17^{16} &\equiv 256 \equiv 74 \pmod{91} \end{aligned}$$

$$\begin{aligned} 17^{91} &\equiv 17^{72+16+2+1} \pmod{91} \\ &\equiv 17^{72} \cdot 17^{16} \cdot 17^2 \cdot 17^1 \pmod{91} \\ &\equiv 1 \cdot 74 \cdot 16 \cdot 17 \pmod{91} \\ &\equiv 20128 \pmod{91} \\ &\equiv 17 \pmod{91} \end{aligned}$$

Thus, 91 is a pseudoprime to bases 3 and 17.

Problem 2

Show that $2821 = 7 \times 13 \times 31$ is a Carmichael number.

We need to prove that for all $a \in \mathbb{Z}$ such that $(a, 2821) = 1$, $a^{2821} \equiv a \pmod{2821}$. $2821 = 7 \times 13 \times 31$. Since these are all prime, we can set up 3 congruences with Fermat's little theorem.

$$\begin{aligned} a^6 &\equiv 1 \pmod{7} \\ a^{12} &\equiv 1 \pmod{13} \\ a^{30} &\equiv 1 \pmod{31} \end{aligned}$$

$$\begin{aligned} a^{2821} &\equiv a^{6\cdot 471+1} \pmod{7} \\ &\equiv a^{6\cdot 471} \cdot a^1 \pmod{7} \\ &\equiv 1 \cdot a \pmod{7} \\ &\equiv a \pmod{7} && (1) \\ a^{2821} &\equiv a^{12\cdot 235+1} \pmod{13} \\ &\equiv a^{12\cdot 235} \cdot a^1 \pmod{13} \\ &\equiv 1 \cdot a \pmod{13} \\ &\equiv a \pmod{13} && (2) \\ a^{2821} &\equiv a^{30\cdot 94+1} \pmod{31} \\ &\equiv a^{30\cdot 94} \cdot a^1 \pmod{31} \\ &\equiv 1 \cdot a \pmod{31} \\ &\equiv a \pmod{31} && (3) \end{aligned}$$

Thus, we have our 3 final congruences:

$$\begin{aligned} a^{2821} &\equiv a \pmod{7} \\ a^{2821} &\equiv a \pmod{13} \\ a^{2821} &\equiv a \pmod{31} \end{aligned}$$

We could use the Chinese Remainder Theorem, but it is trivial to see that, since the bases are all the same and the moduli $|2821$, we can simply combine these congruences to get $a^{2821} \equiv a \pmod{2821}$. Thus, 2821 is a Carmichael number.

Problem 3

From the last homework, we know that 25 is a base-7 pseudoprime. Decide whether it is a strong pseudoprime.

From the last homework, we have $7^25 \equiv 7 \pmod{25}$. $25 - 1 = 2^3 \cdot 3$, so we can use the Miller test. We can start with $7^3 \pmod{25}$ and continue square until we reach -1.

$$\begin{aligned} 7^3 &\equiv 343 \pmod{25} \\ &\equiv 325 + 18 \pmod{25} \\ &\equiv 18 \pmod{25} && (1) \\ 7^6 &\equiv 18^2 \pmod{25} \\ &\equiv 324 \pmod{25} \\ &\equiv 24 \pmod{25} \\ &\equiv -1 \pmod{25} && (2) \end{aligned}$$

Since $7^6 \equiv -1 \pmod{25}$, it passes the test, but 25 is not prime, so it is a strong pseudoprime to base 7.

Problem 4

For each statement below, mark "Y" if the statement shows that 25,326,001 cannot be prime. Otherwise, answer "N".

(a) $11251 | 25326001$

(b) $2^{25326001} \equiv 2 \pmod{25326001}$

(c) $7^{25326001} \equiv 5872860 \pmod{25326001}$

(d) $3^{1582875} \equiv 1 \pmod{25326001}$

(e) $43^{1582875} \equiv 12668627 \pmod{25326001}$ and $43^{3165750} \equiv 1 \pmod{25326001}$

(a) Y, if there is factor that isn't 1 or 25,326,001, then it obviously can't be prime.

(b) N, while it seems to pass Fermat's little theorem, it could be a pseudoprime as the converse of a statement is not always true.

(c) Y, if it were prime, then $7^{25326001} \equiv 7 \pmod{25326001}$. Since it doesn't, it fails Fermat's little theorem and thus cannot be prime.

(d) N, 1582875 is 25326001 with all the 2s factored out and is thus the start of the Miller test. Since it is $\equiv 1$ and, thus, passes the test, we can not definitively conclude anything about its primality.

(e) Y, 1582875 is 25326001 with all the 2s factored out and, thus, $43^{1582875} \equiv 12668627 \pmod{25326001}$ is the start of the Miller test. The next step is to square it, which is provided for us: $43^{3165750} \equiv 1 \pmod{25326001}$. We would continue squaring to see if we get a value $\equiv -1$, but since this second step is $\equiv 1$, all future steps will also be $\equiv 1$. Thus, since it is never $\equiv -1$, it fails the Miller test and cannot be prime.