

1. Show that 12 is not pseudoprime by Fermat Test.

Answer: Because $2^{12-1} = 2^{11} = 2048 = 2 \pmod{12}$, so 12 is not a pseudoprime by Fermat Test.

2. Find all the numbers a in Z_{21}^+ satisfying $a^{20} = 1 \pmod{21}$. Identify which of them will pass Square root test.

Answer: There are four numbers in Z_{21}^+ satisfying $a^{20} = 1 \pmod{21}$. They are 1, 8, 13, 20. Fermat Test will succeed to tell that 21 is not a pseudoprime in the other 16 cases.

Square root test will succeed to tell that 21 is not a prime for $a = 5$ or 13: Since $20 = 2^2 \cdot 5$, $h = 2$ and $s = 5$. If $a = 8$, then $x_0 = 8^5 = 8 \pmod{21}$ and $x_1 = x_0^2 = 8^2 = 64 = 1 \pmod{21}$. Since $8 \neq 1$ or $-1 \pmod{21}$, so 21 cannot be a prime. The case for 13 is similar.

3. Suppose a probabilistic TM E will randomly print one of the numbers in $\{1, 2, 3, 4, 5\}$. Given $\epsilon = 0.01$, design E such that the difference of probabilities of printing any two of them is less than 0.01. For any $0 < \epsilon < 1/4$, how to design E ?

Answer: E can be designed such that all its computation can be depicted as a complete binary tree of height 7 ($2^7 - 1$ internal nodes and $2^7 = 128$ leaves). Each internal node is a coin-flip step and each leaf node will print out one number. That is, each leaf node has equal probability to print out one number. For height=7, the probability at each leaf is $1/128 < 0.01$. Since $128/5 = 25.6$, we may assign the first 26 leaves print out 1, the next 26 leaves print out 2, the next 26 leaves print out 3, the next 25 leaves print out 4 and the last 25 leaves print out 5. The difference of probabilities of printing any two of these numbers is by one leaf node, which has probability $1/128 < 0.01$.

In general, design E so that its computation tree is a complete binary tree of height h , where $\epsilon \geq 2^{-h}$, and distribute these 2^h leaf nodes to printing evenly.