QUESTION
For each integer, $n \geq 0$, define $h_n = 2^{2^n} + 1$.

(i) Evaluate $h_0, h)1, h_2, h_3$.

(ii) Show that $\text{HCF}(h_n, h_{n+t}) = 1$ for all $n \geq 0$ and all $t \geq 1$. (Hint: Consider $h_{n+t} - 2$.)

(iii) Use (ii) to give a proof that there exist infinitely many prime numbers.

(Hint: you may assume that every positive integer has a unique factorisation into prime powers.)
ANSWER

(i) We have

$$\begin{aligned} h_0 &= 2^{2^0} + 1 = 2^1 + 1 = 3 \\ h_1 &= 2^{2^1} + 1 = 2^2 + 1 = 5 \\ h_2 &= 2^{2^2} + 1 = 2^4 + 1 = 17 \\ h_3 &= 2^{2^3} + 1 = 2^8 + 1 = 257 \end{aligned}$$

(ii) We have

$$h_n + 1 - 2 = 2^{2^{n+1}} + 1 - 2 = 2^{2^n 2^1} - 2 = (2^{2^n})^{2^t} - 1 = (h_n - 1)^{2^t} - 1$$

which is divisible by h_n, by the binomial theorem. Therefore any common factor of h_n and h_{n+1} must divide 2. Since h_n is odd $\text{HCF}(h_n, h_{n+1}) = 2$ is impossible.

(iii) Suppose that there are only finitely many distinct primes, $p_1, p_2, \ldots p_k$. Let P_n denote the set of primes which appear to a strictly positive exponent in the prime power factorisation of any one of $h_0, h_1 \ldots, h_n$. By (ii) no element of P_m can appear in the prime factorisation of h_{m+1} so that $|P_n| \geq n$ which is impossible for $n > k$.