Problem of the week #11: Solution

Solution 1. Suppose n is special and p_{j+1} is the largest prime not dividing n. Then it cannot share any factor with n, so n must be a factor of $p_{j+1}^2 - 1$, so in particular $n < p_{j+1}^2$.

On the other hand, n is divisible by the primes $p_1, p_2, \cdots, p_j$ so it is divisible by their product, hence their product satisfies $p_1 p_2 \cdots p_j \leq n$.

Putting this together, $p_1 p_2 \cdots p_j < p_{j+1}^2$.

Check when this comparison first fails:

$$\begin{array}{lcl} 2 \cdot 3 & < & 5^2 \\ 2 \cdot 3 \cdot 5 & < & 7^2 \\ 2 \cdot 3 \cdot 5 \cdot 7 & > & 11^2 \end{array}$$

It will follow that $p_1 p_2 \cdots p_k > p_{k+1}^2$ for all $p_{k+1} \geq 11$, since if it holds for one prime p_{k+1} on the right, then for the next prime p_{k+2} we have

$$p_1 p_2 \cdots p_k p_{k+1} > p_1 p_2 \cdots p_k \cdot 4 > p_{k+1}^2 \cdot 4 > p_{k+2}^2.$$

This uses Bertrand's postulate, which implies $p_{k+2} < 2p_{k+1}$.

If the largest prime not dividing n is $p_{k+1} = 7$, then n is a factor $7^2 - 1 = 48$. This would imply 5 is not a factor of n. Therefore n is a factor of one of $5^2 - 1 = 24$ or $3^2 - 1 = 8$ or $2^2 - 1 = 3$.

It turns out the special numbers are precisely the factors of 24:

$$n = 1, 2, 3, 4, 6, 8, 12, 24.$$

To check that one of these numbers n is special, it suffices to check n is a factor of $x^2 - 1$ for relatively prime values $x < n$. This is because if y is any value relatively prime to n and x is its remainder upon division by n then $y^2 - 1 = (x + kn)^2 - 1 = (x^2 - 1) + (2k + n)n$ has n as a factor if $x^2 - 1$ does. Manually check each listed number is special.

Solution 2. The condition that n is a factor of $x^2 - 1$ for values x coprime to n may be restated as $x^2 \equiv 1 \bmod n$ for all units $x \bmod n$.

In other words, the unit group $U(n) := (\mathbb{Z}/n\mathbb{Z})^\times$ has exponent 2.

The Chinese Remainder Theorem indicates $U(n)$ is a direct product of $U(p^v)$ for all prime powers p^v in n's prime factorization. This group, for odd primes p, is cyclic of order $\phi(p^v) = p^{v-1}(p-1)$, hence contains elements order not 2 if $p-1 > 2$, so if n is special it cannot be divisible by any prime $p > 3$ and can only be divisible by 3 at most once. For $p = 2$, we have $U(2^w) \cong \mathbb{Z}_2 \times \mathbb{Z}_{2^{w-2}}$, which contains an element of order 4 if $w - 2 > 1$, so if n is special it can only be divisible by 2 at most 3 times. In conclusion, $n = 2^v 3^w$ with $v \in \{0, 1, 2, 3\}$ and $w \in \{0, 1\}$.