In fact, the only known Fermat primes are

$$3 = 2^{2^0}+1, \quad 5 = 2^{2^1}+1, \quad 17 = 2^{2^2}+1, \quad 257 = 2^{2^3}+1, \text{ and}$$
$$65537 = 2^{2^4}+1.$$

You can show that $n = 2^{2^r}+1$ is not prime by showing that $(n-1 = 2^{2^r})$

$$a^{2^{(2^r)}} \not\equiv_n 1 \quad \text{or}$$
$$a^{2^{(2^r-1)}} \not\equiv_n -1 \quad \text{or}$$
$$\vdots$$

for some a with $(a,n)=1$.

You can show it is prime by showing that

$$a^{2^{(2^r)}} \equiv_n 1 \quad \text{and} \quad a^{2^{(2^r-1)}} \not\equiv_n 1 \quad \text{for some } a!$$

$\left[\ \phi(n-1) = \phi(2^{(2^r)}) = 2^{(2^r-1)}\right.$, so there should be lots of a!$\left.\right]$

Why care about Fermat primes?

Fact (Gauss): a regular polygon with a prime p # of sides can be constructed by ruler and compass $\iff$ p is a Fermat prime!

Conjecture: The above is a complete list of Fermat primes!

$\Longrightarrow q^r \mid m \Longrightarrow q^r \mid \phi(n)$ contrad.

The reverse is also true:

If p is prime ~~and~~ then $\exists$ a st.

$a^{\frac{p-1}{q}} \not\equiv_p 1$ for all prime $q \mid p-1$.

($a^{p-1} \equiv_p 1$ and)

(Why? Later!)

$\exists$ Ex of n's with $n-1$ easy to factor!

$n = 2^k+1$! $\quad n = p \cdot 2^k + 1 \quad p$ prime.

Fact 2^k+1 is prime $\Longrightarrow k = 2^r$ some r

b/c If $k = 2^r \cdot d \quad d$ odd $d \geq 3$, then

$$2^k+1 = (2^{2^r})^d + 1 = (2^{2^r}+1)(\ldots)$$

$$\frac{x^d+1}{x+1} = x^{d-1} - x^{d-2} + \cdots - x + 1.$$

Turns out, ~~the~~ an a which works is 3

Thm Pepin:

$$n = 2^{(2^k)} + 1 \text{ is prime } \iff$$

$$3^{\frac{n-1}{2}} \equiv_n -1 \qquad \text{(Why? Later!)}$$