In fact, the only known Fermat primes are

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

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

\[ a^{2^{2^r}} \not\equiv 1 \mod n \]

\[ a^{2^{2^r} - 1} \not\equiv 1 \mod n \]

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

You can show it is prime by showing that

\[ a^{2^{2^r}} \equiv 1 \mod n \quad \text{and} \quad a^{2^{2^r} - 1} \not\equiv 1 \mod n \]

for some \( a \).

\[ \varphi(n-1) = \varphi(2^{2^r}) = 2^{2^r - 1} \], so there should be \( 2^{2^r} \) bits of \( n \).

---

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!
\[ q | m \Rightarrow q | \phi(n) \text{ contrad.} \]

The reverse is also true:

If \( p \) is prime and \( \not\exists \phi(1) \), then \( \exists a \neq 1 \)

\( (a^{p-1} \equiv 1 \pmod{p}) \quad a^p \equiv 1 \quad \forall \text{ all prime} \)

(Why? Later!) \( q | p^1 \).

---

3. Existence with \( n-1 \) easy to factor:

\[ n = 2^k + 1 \quad n = p \cdot 2^k + 1 \quad p \text{ prime} \]

Fact: \( 2^k + 1 \) is prime \( \Rightarrow k = 2^r \) some \( r \)

b/c If \( k = 2^r d \) and odd \( d \geq 3 \), then

\[ 2^k + 1 = (2^r)^d + 1 = (2^r + 1)(Y) \]

\[ \frac{x^d + 1}{x+1} = x^{d-1} - x^{d-2} + \ldots - x + 1 \]
Theorem: \( n = 2^k + 1 \) is prime \( \iff \quad 3^{\frac{n-1}{2}} \equiv -1 \pmod{n} \) (Why? (Check!))