$2^n - 21,382,107,400,956,509,849$

IS NEVER A PRIME

Joel Spencer

October 1969
The sequence $2^n - a$ for fixed $a$ has been studied by many mathematicians. For $a = +1$, those $2^n - 1$ which are primes are called Mersenne primes. For $a = -1$, the primes of the form $2^n + 1$ are called Fermat primes. Clearly if $a$ is even the only possible prime would be 2. In this note, I find an odd $a$ such that $2^n - a$ is never a prime.

If $p$ is a prime set $x(p) = \min t > 0: 2^t \equiv 1 \pmod{p}$.
So given $x(p)$ we must have $p | 2^{x(p)} - 1$ and $p | 2^t - 1$ for $1 < t < p$. If $x(p)$ is even then $p | 2^{x(p)} - 1$ implies $p | 2^{x(p)} - 1$ and $p | 2^{x(p)} + 1$. It is not difficult to show $x(p) = 2^i$ iff $p | 2^{2^i} + 1$. We get the table:
The last row gives the factorization of $2^{32} + 1$ first found by Fermat. Now the equation $2^n = a(p)$ will either have no solutions or the solution set $n \equiv b(x(p))$ where $2^b = a(p)$. Thus if $a \equiv -1(3)$, $2^n = a(3)$ iff $n \equiv 1(2)$. We have $-1 \equiv 2^{x(p)/2}(p)$ whenever $x(p)$ is even. Set

\[ a \equiv -1 [3, 5, 17, 257, 65537, 64]. \]

Then

\[
\begin{align*}
2^n & = a \quad (3) \text{ iff } n \equiv 1(2) \\
2^n & = a \quad (5) \text{ iff } n \equiv 2(4) \\
2^n & = a \quad (17) \text{ iff } n \equiv 4(8) \\
2^n & = a \quad (257) \text{ iff } n \equiv 8(16) \\
2^n & = a(65537) \text{ iff } n \equiv 16(32) \\
2^n & = a \quad (641) \text{ iff } n \equiv 32(64)
\end{align*}
\]

If

\[ a = +1[6700417] \]

\[ 2^n = a(6700417) \text{ iff } n \equiv 0(64). \]
By the Chinese Remainder Theorem we may solve for a modulo 3, 5, 17, 257, 65537, 641, 6700417. A solution is given as the title. Note all n's satisfy exactly one of the consequences given so all $2^n - a$ are divisible by 3, 5, 17, 257, 65537, or 6700417. One can easily check that $|2^n - a| > 10^{15}$ for all n so it never equals one of these primes.

The following result is due to O. 144.

**Corollary:** There exist infinitely many primes p such that $2^n - p$ is never a prime.

**Proof:** If $a = a_o \pmod{\Delta}$ when $a_o$ is given in the title and $\Delta$ is the product of the primes then $2^n - a$ is always divisible by one of the seven primes. By Dirichlet's Theorem that residue class contains an infinite number of primes. Taking a negative and large $2^n - a$ never equals any of the primes so is never a prime.