PRIMITIVE SOLUTIONS OF $n|2^n + 1$

TOBY BAILEY AND CHRIS SMYTH

Sloane's integer sequence A006521

$$=1, 3, 9, 27, 81, 171, 243, 513, 729, 1539, 2187, 3249, 4617, 6561, 9747, 13203, 13851, 19683, \tag{0.1}$$

$$29241, 39609, 41553, 59049, 61731, 87723, 97641, 118827, 124659, 177147, 185193, 250857, \tag{0.2}$$

$$263169, 292923, 354537, 356481, 373977, 531441, 555579, 752571, \dots \tag{0.3}$$

is the sequence of all integers n such that n divides $2^n + 1$. Here we discuss a sparse subsequence of it, the primitive solutions of $n|2^n + 1$:

$1, 3, 171 = 3^2 \times 19, 13203 = 3^4 \times 163, 97641 = 3^2 \times 19 \times 571, 354537 = 3^5 \times 1459, 2354697 = 3^3 \times 87211, \dots$.

Proposition 1. (a) *If $p|n$ and $n|2^n + 1$ then $pn|2^{pn} + 1$. (Here p need not be prime, but might as well be!)*

(b) *If $n|2^n + 1$ and $m|2^m + 1$ then $\ell|2^\ell + 1$, where $\ell = \mathrm{lcm}(n, m)$.*

Proof. (a) Clearly $p > 2$. Write and $M = 2^n$, so that

$$2^{pn} + 1 = (M + 1)(M^{p-1} - M^{p-2} + ... - M + 1).$$

Now $n|(M + 1)$, and

$$M^{p-1} - M^{p-2} + ... - M + 1 \equiv (-1)^{p-1} - (-1)^{p-2} + ... - (-1) + 1 = p \equiv 0 \pmod p,$$

so that $pn|2^{pn} + 1$.

(b) Let $\ell = nt$. Then, as t odd, $2^{nt} + 1$ is divisible by $M + 1$, and so by n. Similarly, it is divisible by m, and so by ℓ.

□

We call an n with $n|2^n + 1$ *primitive* if it is not generated from smaller members of the sequence by using either Proposition 1(a) or (b).

Examples: 9 is not primitive, by (a), and $250857 = 3^4 \times 19 \times 163$ is not primitive, being generated by (b) from $171 = 3^2 \times 19$ and $13203 = 3^4 \times 163$.

The following result is known. See for instance the exam at
`http://www.math.ubc.ca/~boyd/math537/`

Proposition 2. *For $n > 1$ and $n|2^n + 1$ we have $3|n$.*

Proof. For $p|n$, $2^{2n} \equiv 1 \pmod p$, $2^{p-1} \equiv 1 \pmod p$ so as p odd, $2^{2(n,(p-1)/2)} \equiv 1 \pmod p$. Now let p be smallest prime factor of n. Then $(n, (p-1)/2) = 1$, $2^2 \equiv 1 \pmod p$, $p = 3$. □

Proposition 3. *Every element $n > 3$ of* A006521 *is divisible by* 9*, and if n is not a power of* 3 *with $3^k||n$ then n also divisible by a prime $p > 3$ such that $p|2^{3^k}+1$.*

Corollary 4. *Every element $n > 9$ of* A006521 *is divisible either by* 27 *or by* $9 \times 19 = 171$*.*

Proof of Proposition 3. Let $n = 3^k m$, and $p|m$, p prime, minimal. Then $2^{2n} \equiv 1 \pmod{3^k p}$, $2^{2.3^{k-1}(p-1)} \equiv 1 \pmod{3^k p}$ (Euler's Theorem), so $2^{2(n,3^{k-1}(p-1))} \equiv 1 \pmod{3^k p}$,

$$2^{2.3^{k-1}(3m,p-1)} \equiv 1 \pmod{p}$$

. Now $(3m, p-1) = (3, p-1) = 1$ or 3. If $= 1$ get $2^{2\cdot 3^{k-1}} \equiv 1 \pmod{p}$. If $= 3$ get $2^{2\cdot 3^k} \equiv 1 \pmod{p}$, so the latter congruence certainly holds. As 2 must have even order $\pmod{p}$ have $2^{3^k} \equiv -1 \pmod{p}$. If $k = 1$ get $2^3 \equiv -1 \pmod{p}$, a contradiction. □

Proof of Corollary. If $k = 2$ get $p|513 = 27 \times 19$, $p = 19$. So either

- $k = 2$ and $19|n$, i.e. $171|n$

  or
- $k \geq 3$, i.e. $27|n$.

□

By separating the cases $k = 2$, $k = 3$, $k = 4$ and $k \geq 5$, the same argument gives the following.

Corollary 5. *Every element n of* A006521 *not a power of* 3 *is divisible by at least one of* $171 = 3^2 \times 19$*,* $243 = 3^5$*,* $13203 = 3^4 \times 163$*,* $2354697 = 3^3 \times 87211$*,* $10970073 = 3^4 \times 135433$ *or* $22032887841 = 3^4 \times 272010961$*.*

For computational purposes, one then only has to search a proportion $1/171 + 1/243 + 1/13203 + \ldots$ of the odd integers to find the non-power-of-3 n. If one were to go further, for instance replacing '$k \geq 5$' by '$k = 5$ or $k \geq 6$', then in the above list one replaces 243 by $3^6 = 729$, $3^5 \times 1459 = 354537$, $3^5 \times 139483 = 33894369$, $3^5 \times 10429407431911334611 = 2534346005954454310473$ and $3^5 \times 918125051602568899753 = 223104387539424242639979$. Doing this, the proportion of odd integers to be searched is $1/171 + 1/729 + 1/13203 + \ldots$, a further 27% saving in integers to be tested.

If one restricts the above results to primitive n then the condition that n not be a power of 3 can clearly be replaced by the condition $n > 3$.