# Finding primes $p$ for which $(p-1)/2 - \phi(p-1) = k$

T. D. Noe

November 13, 2007

Sloane's OEIS [3] sequence A098006 concerns the difference between the number of quadratic nonresidues (mod $p$) and the primitive roots (mod $p$) for odd primes $p$. This difference is expressed as

$$f(p) = \frac{p-1}{2} - \phi(p-1), \tag{1}$$

where $\phi$ is Euler's totient function.

For a given number $k \geq 0$, we want to find primes $p$ such that $f(p) = k$. As proved by Luca and Walsh [1], there are an infinite number of $k$ for which this is not possible. This short note shows that, in general, the search can be limited to primes $p \leq 1 + k^2$.

For any odd prime $p$, we can factor $p-1$ into even and odd parts:

$$p - 1 = 2^\alpha\ m$$

with $m$ odd. By ignoring the Fermat primes (3, 5, 17, 257, and 65537), which produce $f(p) = 0$, we can take $m > 1$. Thus, equation (1) becomes

$$f(p) = 2^{\alpha-1}(m - \phi(m)).$$

Note that the factor $m - \phi(m)$ is odd because $m$ is odd and $m > 1$.

Let's also factor $k$ into even and odd parts: $k = 2^\beta\ k_o$. If $k = f(p)$ for some prime $p$, then the even and odd parts must be equal, producing the two equations

$$\beta = \alpha - 1 \quad \text{and} \quad k_o = m - \phi(m). \tag{2}$$

For the second equation in (2), we have two possibilities to consider, $k_o = 1$ and $k_o > 1$, which are discussed below.

It is easy to see that the case $k_o = 1$, which occurs when $k = 2^\beta$, is solved by $m$ any odd prime. In this case, the possible primes $p$ have the form $p = 1 + m\ 2^{\beta+1} = 1 + 2mk$. It is very easy to compute the least prime for which $f(p) = k$: merely check the primality of $1 + 2mk$ as $m$ goes through increasing odd primes. For $k = 1, 2, 4, 8, 16, 32, 64, 128, 256$, we easily obtain the primes $p = 7, 13, 41, 113, 97, 193, 641, 769, 11777$. Although no proof is known that a prime exists whenever $k$ is a power of 2, using probabilistic arguments it is easy to show that an infinite number of primes are expected for each such $k$. We have computed the least prime for all powers $\beta \le 1000$. For all $\beta > 3$, we found a prime $p \le 1 + k^2$. See new sequences A134854 and A134855.

For the second case, $k_o > 1$, there are only a finite number of solutions to the equation

$$m - \phi(m) = k_o \tag{3}$$

because $m$ must be composite and the fact from Sierpinski [2, page 231] that

$$m - \phi(m) \ge \sqrt{m} \tag{4}$$

for all composite $m$. Hence, we must have $m \le k_o^2$. So the possible primes are of the form $p = 1 + m\ 2^{\beta+1}$ with $m$ a solution to equation (3). Luca and Walsh show that for some values of $k$ it is possible that these values of $p$ are all composite. The values of $k$ for which there are no primes are listed in OEIS sequence A098047.

(Although the above analysis seems to show that the largest prime will have the form $1+2k_o^2$, this will never be the case because (1) the bound in inequality (4) is sharp only for the squares of odd primes and (2) $1 + 2k_o^2$ is composite when $k_o$ is an odd prime greater than 3. If we exclude the squares of odd primes, then inequality (4) becomes

$$m - \phi(m) \ge 2\sqrt{m}$$

from which we can conclude that $m \le k_o^2/4$ instead of $m \le k_o^2$.)

In conclusion, we have discovered that finding the primes $p$ for which $f(p) = k$ for a given $k$ is easily accomplished. Numerical experiments have shown that, if such a prime $p$ exists, then $p \le 1 + k^2$ except for $k = 0$, 1, 2, 3, 4, and 8. This numerical work is supported by the analysis shown above. The graph of the new sequence A134765, which lists the least $p$ for each $k$, clearly shows the many $k$ for which $p = 1 + k^2$.

# References


[1] Florian Luca and P. G. Walsh, *On the number of nonquadratic residues which are not primitive roots*, Colloq. Math., 100 (2004), 91-93 .

[2] W. Sierpinski, *Elementary Theory of Numbers*, Warsaw, 1964.

[3] N. J. A. Sloane, *The On-Line Encyclopedia of Integer Sequences*, published electronically at www.research.att.com/∼njas/sequences.