MATHEMATICS OF COMPUTATION
Volume 88, Number 317, May 2019, Pages 1251–1260
https://doi.org/10.1090/mcom/3378
Article electronically published on September 6, 2018

QUADRATIC NON-RESIDUES THAT ARE NOT PRIMITIVE ROOTS

TAMIRU JARSO AND TIM TRUDGIAN

ABSTRACT. We prove that any prime p satisfying $\phi(p-1) \leq (p-1)/4$ contains two consecutive quadratic non-residues modulo p neither of which is a primitive root modulo p. This improves on results by Luca et al. and Gun et al.

1. INTRODUCTION

Let p be an odd prime: it is well known that there are $(p-1)/2$ quadratic non-residues and $\phi(p-1)$ primitive roots modulo p. Therefore, provided[1] that $\phi(p-1) < (p-1)/2$ there will be some quadratic non-residues that are not primitive roots. Following Gun et al. [3] we denote these as QNRNPs. Luca et al. [4], building on work by Gun et al. [2], showed that for any fixed $\epsilon \in (0, \frac{1}{2})$ one can always find n consecutive QNRNPs modulo p provided that

$$\frac{\phi(p-1)}{p-1} \leq \frac{1}{2} - \epsilon, \quad p \geq \max\left\{ n^2 \left(\frac{4}{\epsilon}\right)^{2n}, n^{651n \log\log(10n)} \right\}. \tag{1}$$

Choosing $n = 2$ in (1) means that one requires that $p \geq 10^{430}$ irrespective of the value of ϵ. By contrast, Cohen, Oliveira e Silva, and Trudgian [1] proved that all $p > 61$ have three consecutive primitive roots. The multiplicative structure of primitive roots makes their detection much easier than that of QNRNPs.

Gun et al. [3] proved that for $n = 2$ and $\epsilon = \frac{1}{3}$ one may remove the lower bound on p in (1). This then yields a complete result for those primes p satisfying $\phi(p-1) \leq (p-1)/6$. It is straightforward to check that $p = 300\,690\,391$ is the smallest such prime.

One could improve this by furnishing a complete result for some $\epsilon < \frac{1}{3}$. The goal of this paper is to take $\epsilon = \frac{1}{4}$ and to prove

Theorem 1. *Any p satisfying $\phi(p-1) \leq (p-1)/4$ contains two consecutive QNRNPs.*

We note that the sequence of such primes starts with $211, 331, 421, 631, \ldots$.

Throughout this paper we use the following notation: $\omega(n)$ is the number of distinct prime divisors of n, $\mu(n)$ is the Möbius function, and q_i is the ith prime.

The outline of this paper is as follows. In Sections 2 and 3 we treat large and small values of $\omega(p-1)$. In Section 4, we present computational details that complete

Received by the editor October 11, 2017, and, in revised form, March 8, 2018.
2010 *Mathematics Subject Classification.* Primary 11A07; Secondary 11N35, 11N69.
The second author was supported by Australian Research Council Future Fellowship FT160100094.

[1]Indeed, the only time that $\phi(p-1) = (p-1)/2$ is when p is a Fermat prime, that is, $p = 2^{2^n}+1$.

the proof of Theorem 1. We conclude, in Section 5, with some possible extensions and conjectures.

2. A criterion for two consecutive QNRNPs

For brevity, we merely state some necessary results from [4]. For k a positive integer, let

$$\theta_k(p) = -\frac{1}{2} - \sum_{\nu=1}^{2k} \sum_{\substack{d|p-1 \\ \omega(d)=\nu}} \frac{\mu(d)}{d}. \tag{2}$$

The last displayed equation in [4, p. 101] implies the following criterion.

Proposition 1. *Let k be a positive integer and let $\theta_k(p)$ be as in* (2)*. If*

$$p\theta_k(p)^2 - 2p^{1/2}\left\{\theta_k(p)\sum_{\nu=1}^{2k}\binom{\omega(p-1)}{\nu} + \left(\sum_{\nu=1}^{2k}\binom{\omega(p-1)}{\nu}\right)^2\right\} > 0, \tag{3}$$

then there exist two consecutive QNRNPs modulo p.

We proceed in the next three sections to use Proposition 1 to prove Theorem 1. We break this proof into three cases, depending on the size of $\omega(p-1)$.

2.1. **Case 1: $\omega(p-1) \geq 48$.** As in [4] we bound the sums in (3) by noting that for $\omega(p-1) \geq 2$ we have $\sum_{\nu=1}^{2k}\binom{\omega(p-1)}{\nu} \leq \omega(p-1)^{2k}$. We now seek to bound $\theta_k(p)$. We have[2]

$$\theta_k(p) = -1/2 + \sum_{\nu\geq 2k+1}\sum_{\substack{d|p-1 \\ \omega(d)=\nu}}\frac{\mu(d)}{d} - \sum_{\substack{d|p-1 \\ d>1}}\frac{\mu(d)}{d} = \frac{1}{2} - \frac{\phi(p-1)}{p-1} + \sum_{\nu\geq 2k+1}\sum_{\substack{d|p-1 \\ \omega(d)=\nu}}\frac{\mu(d)}{d}. \tag{4}$$

To bound (4) we note that

$$\left|\sum_{\nu\geq 2k+1}\sum_{\substack{d|p-1 \\ \omega(d)=\nu}}\frac{\mu(d)}{d}\right| \leq \sum_{\nu\geq 2k+1}\sum_{\substack{d|p-1 \\ \omega(d)=\nu \\ d \text{ squarefree}}}\frac{1}{d} \leq \sum_{\nu\geq 2k+1}\frac{1}{\nu!}P^\nu, \tag{5}$$

where

$$P = \sum_{\substack{j|p-1 \\ j\text{prime}}}\frac{1}{j} \leq \sum_{q\leq q_{\omega(p-1)}}\frac{1}{q}, \tag{6}$$

since for $\omega(p-1) = n$ we have that $p \geq 2\cdot 3\cdot 5\cdots q_{\omega(p-1)} + 1$. To estimate (6) we use the following results:

$$\omega(n) \leq \frac{1.385\log n}{\log\log n} \quad (n\geq 3), \qquad \sum_{p\leq x}\frac{1}{p} \leq \log\log x + 0.262 + \frac{1}{\log^2 x} \quad (x\geq 2), \tag{7}$$

$$p_n \leq n(\log n + \log\log n) \quad (n\geq 6),$$

which are respectively [6, Thm. 10] and [7, (3.20) and (3.13)]. We also use the inequality $\nu! \geq (\nu/e)^\nu$, which is valid for all $\nu \geq 1$. Although sharper versions of

[2] We have corrected a slight misprint in [4]: their sum is over $\nu \geq 2k$ instead of $\nu \geq 2k+1$.

these inequalities are available, the present ones are sufficient for our purposes. For any $k \geq eP$ we have

$$\sum_{\nu \geq 2k+1} \frac{1}{\nu!} P^{\nu} \leq \sum_{\nu \geq 2k+1} \left(\frac{eP}{\nu}\right)^{\nu} \leq \sum_{\nu \geq 2k+1} 2^{-\nu} \leq 2^{-2k}. \tag{8}$$

Therefore taking $k = \max\{[eP]+1, \log(2/\epsilon)/(2\log 2)\}$ we ensure that the sum in (8) is at most $\epsilon/2$. This shows, from (4) and from the assumption that $\phi(p-1)/(p-1) \leq \frac{1}{2} - \epsilon$, that $\frac{\epsilon}{2} \leq \theta_k(p) \leq 1$. Therefore, our criterion in (3) becomes

$$p^{1/2} > \frac{8\left(\omega(p-1)^{2k} + \omega(p-1)^{4k}\right)}{\epsilon^2}, \qquad k = \max\{[eP]+1, \log(2/\epsilon)/(2\log 2)\}.$$

We now insert our bounds for (7). These bound $\omega(p-1)$, P, and hence k. For $\epsilon = 1/4$, a quick computer check verifies Theorem 1 for all p with $\omega(p-1) \geq 48$. Before considering the remaining cases in the next section, we briefly dispense with the case $\omega(p-1) = 1$.

When $\omega(p-1) = 1$ the bound for $\theta_k(p)$ in (4) reduces to $\theta_k(p) = \frac{1}{2} - \phi(p-1)/(p-1) \geq \epsilon$. Taking $\epsilon = \frac{1}{4}$ and inserting this into (3) proves the existence of two consecutive QNRNPs provided that $p > 1600$. It is easy to check that there are no $p < 1600$ satisfying both $\phi(p-1) \leq (p-1)/4$ and $\omega(p-1) = 1$.

3. Case 2: $15 \leq \omega(p-1) \leq 47$

Since we need only consider $\omega(p-1) \leq 47$, the sum in (5) is finite, whence there is no concern over its convergence. This enables us to choose any $k = 2, 3, \ldots, \omega(p-1)$: we shall choose the value of k that minimises the required size of p. We no longer need the estimates in (7), and therefore we can use (5) in (4) to bound $\theta_k(p)$. Since $\mu(d) = (-1)^{\omega(d)}$ on square-free d we can make a small saving[3] by removing all the terms with even ν in (4). We therefore obtain

$$\theta_k(p) \geq \epsilon - \sum_{\substack{\nu=2k+1 \\ \nu \text{ odd}}}^{\omega(p-1)} \frac{1}{\nu!} \left(\frac{1}{2} + \frac{1}{3} + \cdots + \frac{1}{q_{\omega(p-1)}}\right)^{\nu}.$$

We note that we only need this lower bound since (3) is increasing in $\theta_k(p)$ provided that

$$\theta_k(p) > \frac{\sum_{\nu=1}^{2k} \binom{\omega(p-1)}{\nu}}{p^{1/2}}. \tag{9}$$

Therefore, we have two consecutive QNRNPs modulo p if

$$p > 4\frac{\left(\sum_{\nu=1}^{2k} \binom{\omega(p-1)}{\nu} \left\{\epsilon - \sum_{\substack{\nu=2k+1 \\ \nu \text{ odd}}}^{\omega(p-1)} \frac{1}{\nu!} \left(\frac{1}{2} + \frac{1}{3} + \cdots + \frac{1}{q_{\omega(p-1)}}\right)^{\nu}\right\} + \left\{\sum_{\nu=1}^{2k} \binom{\omega(p-1)}{\nu}\right\}^2\right)^2}{\left\{\epsilon - \sum_{\substack{\nu=2k+1 \\ \nu \text{ odd}}}^{\omega(p-1)} \frac{1}{\nu!} \left(\frac{1}{2} + \frac{1}{3} + \cdots + \frac{1}{q_{\omega(p-1)}}\right)^{\nu}\right\}^4}. \tag{10}$$

[3]One could make slight additional savings by using some combinatorial identities involving the binomial coefficients; we have not pursued this here.

subject to

$$\epsilon - \frac{\sum_{\nu=1}^{2k}\binom{\omega(p-1)}{\nu}}{p_0^{1/2}} - \sum_{\substack{\nu=2k+1\\ \nu \text{ odd}}}^{\omega(p-1)} \frac{1}{\nu!}\left(\frac{1}{2}+\frac{1}{3}+\cdots+\frac{1}{q_{\omega(p-1)}}\right)^{\nu} > 0, \quad (p \geq p_0). \tag{11}$$

We now proceed as follows. For a given value of $\omega(p-1) \in [15, 47]$ we check whether for some $k \in [1, \omega(p-1)]$ we satisfy (10) and (11) for $p \geq 2\cdot 3\cdots q_{\omega(p-1)}+1$.

If so, we have verified Theorem 1 for this particular value of $\omega(p-1)$. For example when $\omega(p-1) = 47$ we have $p-1 > 2\cdot 3\cdots q_{47} > 10^{84}$. For $k = 3$ we find that (11) is satisfied and that (10) is true except possibly when $p < 3.7 \cdot 10^{29}$. Since this is less than 10^{84} we conclude that Theorem 1 is true for $\omega(p-1) = 47$. Similarly for $28 \leq \omega(p-1) \leq 47$ we find we may take $k = 3$ and for $15 \leq \omega(p-1) \leq 27$ we may take $k = 2$.

4. Case 3: $2 \leq \omega(p-1) \leq 14$

For each value of $\omega(p-1)$ we can choose the k that minimises the right side of (10). We have now created an interval that needs further checking. We summarise these intervals in Table 1 below: in each case except the last the optimal value is $k = 2$.

Table 1. Intervals of p for a given value of $\omega(p-1)$.

$\omega(p-1)$	Interval
14	$(1.30 \cdot 10^{16}, 4.3 \cdot 10^{16})$
13	$(3.04 \cdot 10^{14}, 1.07 \cdot 10^{16})$
12	$(7.42 \cdot 10^{12}, 2.47 \cdot 10^{15})$
11	$(2.00 \cdot 10^{11}, 5.12 \cdot 10^{14})$
10	$(6.46 \cdot 10^{9}, 9.33 \cdot 10^{13})$
9	$(2.23 \cdot 10^{8}, 1.5 \cdot 10^{13})$
8	$(9.69 \cdot 10^{6}, 2 \cdot 10^{12})$
$2 \leq \omega(p-1) \leq 7$	$(2, 2.2 \cdot 10^{11})$

To illustrate the computational part of the proof of Theorem 1 we break the proof into two sub-cases based on the values of $\omega(p-1)$ listed in Table 1.

4.1. **When $2 \leq \omega(p-1) \leq 9$.** In this case we checked the two consecutive QNRNPs directly by finding primes p satisfying $\phi(p-1) \leq (p-1)/4$ in each interval in Table 1 for $2 \leq \omega(p-1) \leq 9$.

We coded this using the "primesieve" C/C++ library's highly optimised sieve of Eratosthenes implementation and the gmp library implementation, which generates primes. The check for two consecutive QNRNPs, shown in Algorithm 3, was implemented in C++ and gmp. We give a partial list of these primes with their two consecutive QNRNPs in Table 2.

TABLE 2. Partial list of primes with $2 \le \omega(p-1) \le 9$ and their two consecutive QNRNPs.

$I_9 = (2.23 \cdot 10^8, 1.5 \cdot 10^{13})$		$I_8 = (9.69 \cdot 10^6, 2 \cdot 10^{12})$		$I_7 = (5.10 \cdot 10^5, 2.2 \cdot 10^{11})$	
$\omega(p-1) = 9$		$\omega(p-1) = 8$		$\omega(p-1) = 7$	
p	QNRNPs	p	QNRNPs	p	QNRNPs
300690391	14, 15	13123111	14, 15	870871	6, 7
340510171	7, 8	14804791	6, 7	903211	7, 8
358888531	18, 19	16546531	2, 3	930931	2, 3
397687291	2, 3	17160991	6, 7	1138831	6, 7
⋮	⋮	⋮	⋮	⋮	⋮
14999999667511	42, 43	1999999986307	11, 12	219999995671	14, 15
14999999931841	122, 123	1999999987441	106, 107	219999995911	11, 12
14999999943391	11, 12	1999999993291	26, 27	219999997561	78, 79
14999999984971	7, 8	1999999998391	23, 24	219999998011	14, 15

We found that all these primes have at least two consecutive QNRNPs. This proves Theorem 1 for $2 \le \omega(p-1) \le 9$.

4.2. **When** $10 \le \omega(p-1) \le 14$**.** In these cases the intervals in Table 1 are too large to enumerate the primes contained within them. Instead, we follow the approach used in [5] to consider divisibility of $p-1$ by small primes. Note that when $p_i | p-1$ for some prime p_i, we have fewer values to check in our interval. On the other hand, whenever we have $p_j \nmid p-1$, the lower bound on p increases. Once we readjust our P in (6), our upper bound decreases, whence the size of the interval decreases. Proceeding in this way we shrink the interval to some manageable width such that we can enumerate the remaining cases. We shall call this process of considering $p_i | p-1$ and $p_j \nmid p-1$ the *prime divisor tree*.

For example, when $\omega(p-1) = 14$ there are $3.0 \cdot 10^{16}$ numbers in the interval to check: this is unmanageable. We start with $p-1 \in (1.3 \cdot 10^{16}, 4.3 \cdot 10^{16})$. We immediately deduce that $2, 3, \ldots, 13$ all divide $p-1$. For instance, take 13: if $13 \nmid (p-1)$, then

$$p - 1 \ge 2 \cdot 3 \cdot 5 \cdot 7 \cdot 11 \cdot 17 \cdot \cdots \cdot q_{15} > 4.7 \cdot 10^{16}.$$

However, we only needed to check $p-1 \le 4.3 \cdot 10^{16}$, and this is a contradiction. All we have done here is to increase the lower bound. We cannot, at this stage, deduce that 17 divides $p-1$. For that we need to look at the upper bound on our interval.

Suppose that $17 \nmid (p-1)$. Then, as before, we can increase our lower bound to show that we need only check those p with $p-1 \ge 3.6 \cdot 10^{16}$. We now change our upper bound by altering P in (6). Since 17 cannot divide $p-1$, and since p must have 14 prime factors, we delete $1/17$ from P and replace it by $1/q_{15}$, that is, the reciprocal of the 15th prime. We find that we need only check $p < 3.2 \cdot 10^{16}$. This is a contradiction since our lower bound was $3.6 \cdot 10^{16}$.

We therefore deduce that $2, 3, 5, 7, 11, 13, 17$ primes all divide $p-1$. The product of these primes is $D = 510510$. Hence $p - 1 = D \cdot n \in (1.3 \cdot 10^{16}, 4.3 \cdot 10^{16})$. This gives $5.9 \cdot 10^{10}$ values of n to check–a substantial saving on the $3.0 \cdot 10^{16}$ we had earlier.

We note that we can keep splitting into deeper sub-cases if required. For example, we could consider $7 \nmid (p-1)$ *and* $11 \nmid (p-1)$. When we have k such cases we say that we have gone down the prime divisor tree to *level* k.

Suppose we now wish to enumerate the $5.9 \cdot 10^{10}$ possible exceptions that we have found above. We proceed to compute the following:

(1) Find all primes p such that $p-1 = D \cdot n \in (1.3 \cdot 10^{16}, 4.3 \cdot 10^{16})$.
(2) Check that $\omega(p-1) = 14$.
(3) Check $\phi(p-1) \leq (p-1)/4$. Primes satisfying these first three steps will give us an *initial list* of primes.
(4) Check this initial list against the sieving criteria equations (10) and (11).
(5) Place the p on our initial list that do not satisfy (10) and (11) into a *final list* of primes.
(6) Finally, check this *final list* of primes for two consecutive QNRNPs.

We now present the pseudocode of the three algorithms used in the proof of Theorem 1.

(1) **Prime divisor tree**: This algorithm examines whether small primes p_i divide $p-1$.

Algorithm 1: Prime divisor tree

Data: $L = \{2, 3, 5, 7, \ldots, n = q_{\omega(p-1)}\}$ list of distinct primes.
Input: Let $p-1 \in I$ where I is an interval $I = (lower, upper)$ see Table 1.
Result: $D = \prod_{p_i \in M}(p_i)$ where p_i are primes which divide $p-1$.

Function *PrimeDivisorTree* $(m = \omega(p-1))$
  $M = [2]$ ▷ since 2 divides $p-1$ always
  for $i \in L$ **do**
    let $t = i$
    assume $t \nmid p-1$
    $L' = (L - set(t))$, ▷ remove t from the list L
    $x = q_{\omega((p-1)+1)}$, ▷ the $(n+1)$th prime
    append x to L'
    $Prod = \prod_{p_i \in L'}(p_i)$ ▷ product of p_i where $p_i \in L'$
    $d = \sum_{p_i \in L'}(1/p_i)$ ▷ the criteria equation P (5).
    Evaluate the sieving criteria equation (10) below by setting:
    $\omega(p-1) = m, d, k = 2, \epsilon = \frac{1}{4}$

$$R = 4\frac{\left(\sum_{\nu=1}^{2k}\binom{\omega(p-1)}{\nu}\left\{\epsilon - \sum_{\substack{\nu=2k+1 \\ \nu \text{ odd}}}^{\omega(p-1)} \frac{1}{\nu!}(d)^{\nu}\right\} + \left\{\sum_{\nu=1}^{2k}\binom{\omega(p-1)}{\nu}\right\}^2\right)^2}{\left\{\epsilon - \sum_{\substack{\nu=2k+1 \\ \nu \text{ odd}}}^{\omega(p-1)} \frac{1}{\nu!}(d)^{\nu}\right\}^4}$$

    if $Prod > R$ **and** $Prod \in I$ **then**
      append t to M
    else
      $Prod \notin I$ ▷ Contradiction! t must divide $p-1$.
      append t to M
  $D = \prod_{p_i \in M}(p_i)$, ▷ product of $p_i \in M$ where $p_i \mid p-1$.
  return D

For completeness, we give the list of primes dividing $p-1$ for each respective $\omega(p-1)$. The output of this algorithm is summarised in Table 3.

TABLE 3. List of primes dividing $p-1$ with respect to $\omega(p-1)$.

Primes which must divide $p-1$ for each $\omega(p-1)$				
$\omega(p-1)$	$p_i \nmid p-1$	$p_i \mid p-1$	Tree level	$D=\prod_{p_i\in M}(p_i)$
14		$2,3,5,7,11,13,17$	0	510150
13	5	$2,3,7,11,13,17,19,23,31$	1	40112098026
13	7	$2,3,5,11,13,17,19$	1	1385670
12	$3,5$	$2,7,11,13,17,19,23,29,31$	2	13370699342
12	$3,7$	$2,5,11,13,17,19,23,29,31$	2	9550499530
12	$3,11$	$2,5,7,13,17,19,23,29,31$	2	6077590610
12	$3,13$	$2,5,7,11,17,19,23$	2	5720330
11	$3,5,7$	$2,11,13,17,19,23,29$	3	61616126
11	$3,5,11$	$2,7,13,17,19,23,29$	3	39210262
11	$3,5,13$	$2,7,11,17,19,23$	3	1144066
10	$3,5,7,11$	$2,13,17,19$	4	8398

The output of Algorithm 1 in Table 3 will be used in the next algorithm to find the initial list of primes.

(2) **Sieving the initial list of primes**: We use this algorithm to check the initial list against the sieving criteria in (10) and (11). Primes that do not satisfy the sieving criterion will go in the final list of primes. The final lists are presented in Table 4.

Algorithm 2: Sieving for initial list of primes

Data: Interval $I=(lower, upper)$ in Table 1
Input: $D=\prod p_i$, where $p_i \nmid p-1$ from Algorithm 1
Result: Return initial list of primes for interval I

```
Function Sieving algorithm
    Find initial number m such that D | m where m is the smallest number in the
     interval I, i.e., lower ≤ m.
    S ⟵ ∅                                   ▷ create empty list
    set w ∈ {10, 11, 12, 13, 14}
    for n = m;  n ≤ upper;  n = n + D do
        Assert n%D == 0
        p = n + 1
        if Isprime(p) then
            if ω(p − 1) == w then
                if φ(p−1)/(p−1) ≤ 1/4 then
                    append p to S           ▷ save the initial list of primes.
    return S
```

TABLE 4. Number of initial and final list of primes found.

The number of initial list of primes and the final list of primes.			
$\omega(p-1)$	$D = \prod p_i$	Size of initial list	Size of final list
14	510150	58	23
13	40112098026	541	355
13	1385670	10836	5101
12	13370699342	918	401
12	9550499530	1226	556
12	6077590610	1870	960
12	5720330	66588	32606
11	61616126	16476	6494
11	39210262	25026	10736
11	1144066	203695	91556
10	8398	1860405	766110

Finally, we use Algorithm 3 to check that the primes in our *final list* have two consecutive QNRNPs.

(3) **Verifying two consecutive QNRNPs algorithm**:

Algorithm 3: Checking QNRNPs

Data: Final list of primes after checking criterion equations (10) and (11)
Input: Read in the final list of primes from Algorithm 2 output
Result: Two consecutive QNRNPs

```
Function Two_consecutive_QNRNPs
    Read in S                          ▷ Read in list of primes list from S
    C ⟵ ∅                                    ▷ create empty list
    for p ∈ S do
        for (n = 2; n ≤ (p − 1)/2; n++) do
            x = legendre_symbol(n, p); ▷ Return quadratic non-residue modulo p
            if x is −1;
            if (x == −1) and (not IsPrimitiveRootModp(n, p)) then
                append p to C
                cons = consecutiveInt(C) ▷ Return consecutive integer from the
                  list C;
                if cons == 2 then
                    2 consecutive QNRNPs found;
                    break;
```

We list some partial results for the case $\omega(p-1) = 13$ and $D = 40112098026$, which corresponds to the second row in Table 4.

Using Algorithm 1 shows that we have $p - 1 = 40112098026 \cdot n = D \cdot n \in I_{13} = (3.04 \cdot 10^{14}, 1.07 \cdot 10^{16})$. We find that there are 541 primes in our initial list. A sample of these is provided in Table 5.

TABLE 5. Initial list of primes when $\omega(p-1)=13$.

Interval $I_{13}=$			$(3.04\cdot 10^{14}, 1.07\cdot 10^{16})$
No.	$\omega(p-1)$	k	primes p
1	13	2	386480064480511
2	13	2	405332750552731
3	13	2	437823549953791
⋮	⋮	⋮	⋮
539	13	2	10691358271555963
540	13	2	10694085894221731
541	13	2	10698097104024331

From this initial list of primes 335 out of 541 do not satisfy equation (10). These are added to the final list of primes to check. Using Algorithm 3 we found that all primes in the final list have two consecutive QNRNPs; see Table 6 below.

TABLE 6. Final list of primes p with $\omega(p-1)=13$.

Interval $I_{13}=$			$(3.04\cdot 10^{14}, 1.07\cdot 10^{16})$	
No.	$\omega(p-1)$	k	primes p	QNRNPs
1	13	2	386480064480511	11, 12
2	13	2	405332750552731	2, 3
3	13	2	437823549953791	6, 7
4	13	2	485155825624471	11, 12
5	13	2	583831586768431	6, 7
6	13	2	586238312649991	6, 7
⋮	⋮	⋮	⋮	⋮
351	13	2	8339505740095531	26, 27
352	13	2	8361166273029571	2, 3
353	13	2	8541269593166311	6, 7
354	13	2	8598228772363231	6, 7
355	13	2	8625906120001171	7, 8

We proceed similarly for the remaining values of $\omega(p-1)$ and, in each case, all primes p satisfying $\frac{\phi(p-1)}{(p-1)} \leq \frac{1}{4}$ have at least two consecutive QNRNPs. This completes the proof of Theorem 1.

5. Concluding remarks

Our result could be extended in two natural directions. First, for a given ϵ obtain the largest N such that all primes p satisfying $\phi(p-1)/(p-1) \leq \frac{1}{2} - \epsilon$ have N consecutive QNRNPs. When $\epsilon = \frac{1}{4}$ the first such prime is 211, which has three consecutive QNRNPs. We conjecture that all primes p with $\phi(p-1)/(p-1) \leq \frac{1}{4}$ have three consecutive QNRNPs.

Second, given an N, find the smallest ϵ such that all primes p with $\phi(p-1)/(p-1) \leq \frac{1}{2} - \epsilon$ have N consecutive QNRNPs. The smallest prime with two consecutive QNRNPs is 31, which corresponds to $\epsilon = 7/30$. We conjecture that all primes p with $\phi(p-1) \leq \frac{4}{15}(p-1)$ have two consecutive QNRNPs.

Acknowledgments

We are grateful to the referees for their helpful comments on the structuring of this paper.

References

[1] S. D. Cohen, T. Oliveira e Silva, and T. Trudgian, *On consecutive primitive elements in a finite field*, Bull. Lond. Math. Soc. **47** (2015), no. 3, 418–426, DOI 10.1112/blms/bdv018. MR3354437

[2] S. Gun, F. Luca, P. Rath, B. Sahu, and R. Thangadurai, *Distribution of residues modulo p*, Acta Arith. **129** (2007), no. 4, 325–333, DOI 10.4064/aa129-4-3. MR2346107

[3] S. Gun, B. Ramakrishnan, B. Sahu, and R. Thangadurai, *Distribution of quadratic non-residues which are not primitive roots*, Math. Bohem. **130** (2005), no. 4, 387–396. MR2182384

[4] F. Luca, I. E. Shparlinski, and R. Thangadurai, *Quadratic non-residues versus primitive roots modulo p*, J. Ramanujan Math. Soc. **23** (2008), no. 1, 97–104. MR2410523

[5] K. McGown, E. Treviño, and T. Trudgian, *Resolving Grosswald's conjecture on GRH*, Funct. Approx. Comment. Math. **55** (2016), no. 2, 215–225, DOI 10.7169/facm/2016.55.2.5. MR3584569

[6] G. Robin, *Estimation de la fonction de Tchebychef θ sur le k-ième nombre premier et grandes valeurs de la fonction $\omega(n)$ nombre de diviseurs premiers de n* (French), Acta Arith. **42** (1983), no. 4, 367–389, DOI 10.4064/aa-42-4-367-389. MR736719

[7] J. B. Rosser and L. Schoenfeld, *Approximate formulas for some functions of prime numbers*, Illinois J. Math. **6** (1962), 64–94. MR0137689

Mathematical Sciences Institute, The Australian National University, ACT 0200, Australia

Email address: tamiru.jarso@anu.edu.au

School of Physical, Environmental and Mathematical Sciences, UNSW Canberra, Australia

Email address: t.trudgian@adfa.edu.au