Springer

Dear Author

Here are the proofs of your article.

- You can submit your corrections **online,** via **e-mail** or by **fax**.
- For **online** submission please insert your corrections in the online correction form. Always indicate the line number to which the correction refers.
- You can also insert your corrections in the proof PDF and **email** the annotated PDF.
- For **fax** submission, please ensure that your corrections are clearly legible. Use a fine black pen and write the correction in the margin, not too close to the edge of the page.
- Remember to note the **journal title**, **article number**, and **your name** when sending your response via e-mail or fax.
- **Check** the metadata sheet to make sure that the header information, especially author names and the corresponding affiliations are correctly shown.
- **Check** the questions that may have arisen during copy editing and insert your answers/corrections.
- **Check** that the text is complete and that all figures, tables and their legends are included. Also check the accuracy of special characters, equations, and electronic supplementary material if applicable. If necessary refer to the *Edited manuscript*.
- The publication of inaccurate data such as dosages and units can have serious consequences. Please take particular care that all such details are correct.
- Please **do not** make changes that involve only matters of style. We have generally introduced forms that follow the journal's style.
- Substantial changes in content, e.g., new results, corrected values, title and authorship are not allowed without the approval of the responsible editor. In such a case, please contact the Editorial Office and return his/her consent together with the proof.
- If we do not receive your corrections **within 48 hours**, we will send you a reminder.
- Your article will be published **Online First** approximately one week after receipt of your corrected proofs. This is the **official first publication** citable with the DOI. **Further changes are, therefore, not possible.**
- The **printed version** will follow in a forthcoming issue.

Please note

After online publication, subscribers (personal/institutional) to this journal will have access to the complete article via the DOI using the URL:

`http://dx.doi.org/10.1007/s12044-013-0123-x`

If you would like to know when your article has been published online, take advantage of our free alert service. For registration and further information, go to: http://www.springerlink.com.

Due to the electronic nature of the procedure, the manuscript and the original figures will only be returned to you on special request. When you return your corrections, please inform us, if you would like to have these documents returned.

AUTH

Metadata of the article that will be visualized in OnlineFirst

1	Article Title	**Distribution of residues and primitive roots**	
2	Article Sub-Title		
3	Article Copyright - Year	**Indian Academy of Sciences 2013** **(This will be the copyright line in the final PDF)**	
4	Journal Name	Proceedings - Mathematical Sciences	
5	Corresponding Author	Family Name	**TANTI**
6		Particle	
7		Given Name	**JAGMOHAN**
8		Suffix	
9		Organization	Central University of Jharkhand, CTI Campus
10		Division	
11		Address	Ratu-Lohardaga Road, Brambe, Ranchi 835 205, India
12		e-mail	jagmohan.t@gmail.com
13	Author	Family Name	**THANGADURAI**
14		Particle	
15		Given Name	**R**
16		Suffix	
17		Organization	Harish-Chandra Research Institute
18		Division	
19		Address	Chhatnag Road, Jhunsi, Allahabad 211 019, India
20		e-mail	thanga@hri.res.in
21	Schedule	Received	16 January 2012
22		Revised	29 October 2012
23		Accepted	
24	Abstract	Given an integer $N\geq 3$, we shall prove that for all primes $p\geq (N-2)^2 4^N$, there exists x in $(\mathbb{Z}/p\mathbb{Z})^*$ such that $x, x+1, \ldots, x+N-1$ are all squares (respectively, non-squares) modulo p. Similarly, for an integer $N\geq 2$, we prove that for all primes $p \geq \exp\left(2^{5.54N}\right)$, there exists an element $x\in(\mathbb{Z}/p\mathbb{Z})^*$ such that $x, x+1, \ldots, x+N-1$ are all generators of $(\mathbb{Z}/p\mathbb{Z})^*$.	
25	Keywords separated by ' - '	Quadratic residues - primitive roots - finite fields	

26 Foot note information

Proc. Indian Acad. Sci. (Math. Sci.)

Distribution of residues and primitive roots

JAGMOHAN TANTI[1] and R THANGADURAI[2]

[1]Central University of Jharkhand, CTI Campus, Ratu-Lohardaga Road, Brambe, Ranchi 835 205, India
[2]Harish-Chandra Research Institute, Chhatnag Road, Jhunsi, Allahabad 211 019, India
E-mail: jagmohan.t@gmail.com; thanga@hri.res.in

MS received 16 January 2012; revised 29 October 2012

Abstract. Given an integer $N \geq 3$, we shall prove that for all primes $p \geq (N-2)^2 4^N$, there exists x in $(\mathbb{Z}/p\mathbb{Z})^*$ such that $x, x+1, \ldots, x+N-1$ are all squares (respectively, non-squares) modulo p. Similarly, for an integer $N \geq 2$, we prove that for all primes $p \geq \exp\left(2^{5.54N}\right)$, there exists an element $x \in (\mathbb{Z}/p\mathbb{Z})^*$ such that $x, x+1, \ldots, x+N-1$ are all generators of $(\mathbb{Z}/p\mathbb{Z})^*$.

Keywords. Quadratic residues; primitive roots; finite fields.

1. Introduction

Let p be a prime number. The study of distribution of quadratic residues and quadratic non residues modulo p has been considered with great interest in the literature. One cannot expect to get consecutive squares in integers as the difference of two squares is at least twice of the least one. But, in modulo p, one can expect to get a string of consecutive squares (which are called quadratic residues). The same is true while dealing with quadratic nonresidues and primitive roots modulo p. Let $\mathbb{Z}/p\mathbb{Z}$ denote the group of residues modulo p and $(\mathbb{Z}/p\mathbb{Z})^*$ the multiplicative group of $\mathbb{Z}/p\mathbb{Z}$. In this paper, we address the following question.

Question. For a given natural number $N \geq 2$, can we find a positive constant $p_0(N)$ depending only on N such that for every prime $p \geq p_0(N)$, there exists an element $x \in (\mathbb{Z}/p\mathbb{Z})^*$ with $x, x+1, x+2, \ldots, x+N-1$ are all quadratic residues (respectively, quadratic non-residues) modulo p? If $p_0(N)$ exists, then can we find the explicit value?

In 1928, Brauer [1] answered the above question and proved the existence of $p_0(N)$ for quadratic residues and non-residues cases using some refinement of van der Warden's theorem in combinatorial number theory. Therefore, in his proof, the constant $p_0(N)$ depends on the van der Warden number, which is very difficult to calculate for all N. For instance, recently, Luca and Thangadurai [8] proved that for all primes $p \geq \exp\left(2^{2^{2^{N^2+10}}}\right)$, there exists x such that $x, x+1, \ldots, x+N-1$ are all quadratic residues modulo p, using Gowers [3] bound for van der Warden theorem.

For a given prime p, the set of all non-residues modulo p can be further divided into two classes, namely the set of all primitive roots modulo p (or generators of $(\mathbb{Z}/p\mathbb{Z})^*$) and non-residues which are not primitive roots modulo p.

In 1956, Carlitz [2] answered the above question for the set of all primitive roots modulo p and proved the existence of $p_0(N)$ in this case. This was independently proved by Szalay [12,13]. Recently, Gun *et al* [4,5] and Luca *et al* [7] answered the above question for the complementary case and gave an explicit value of $p_0(N)$ in that case.

In this article, we shall prove the following theorems.

Theorem 1.1. *Let p be a prime. For all $p \geq 7$ (respectively for $p \geq 5$), there is a consecutive pair of quadratic residues (respectively for p nonresidues) modulo p.*

Theorem 1.2. *Let $N \geq 3$ be any positive integer. Then for all primes $p > (N-2)^2 4^N$, we can find N consecutive quadratic residues (respectively quadratic nonresidues) modulo p.*

Theorem 1.3. *Let $N \geq 2$ be any positive integer. Then for all primes $p \geq e^{2^{5.54N}}$, we can find N consecutive primitive roots modulo p.*

Let p be an odd prime. It has been conjectured [10] that there exists an integer $g \leq p-1$ which is a primitive root modulo p and which is relatively prime to $p-1$. In 1976, Hausman [6] proved this conjecture for all sufficiently large primes p without giving an explicit bound. Here, we compute an explicit bound.

Theorem 1.4. *Let p be a prime number such that $p > e^{110.8} \sim 1.318 \times 10^{48}$. Then there exists an integer $1 < g \leq p-1$ such that g is a primitive root modulo p and $(g, p-1) = 1$. In particular, odd primitive root modulo p exists.*

2. Preliminaries

Lemma 2.1.

(i) *For any integer $n > 90$, we have*

$$\phi(n) > \frac{n}{\log n},$$

where $\phi(n)$ is the Euler Φ-function.

(ii) *Let $\omega(n)$ denote the number of distinct prime divisors of n. Then we have*

$$\omega(p-1) \leq (1.385)\frac{\log p}{\log\log p}$$

for all primes $p \geq 5$.

The first result was proved by Moser [9] in 1951 and the second result can be seen in page 167 of [11].

Lemma 2.2. *Let N be any positive integer. Then*

$$\binom{N}{2} + 2\binom{N}{3} + \cdots + (r-1)\binom{N}{r} + \cdots + (N-1) = (N-2)2^{N-1} + 1.$$

Proof. Differentiating

$$(1+x)^N = 1 + \binom{N}{1}x + \binom{N}{2}x^2 + \cdots + \binom{N}{r}x^r + \cdots + x^N, \tag{2.1}$$

we get

$$N(1+x)^{N-1} = \binom{N}{1} + 2\binom{N}{2}x + \cdots + r\binom{N}{r}x^{r-1} + \cdots + Nx^{N-1}. \tag{2.2}$$

Substituting $x = 1$, we get

$$2^N = 1 + \binom{N}{1} + \binom{N}{2} + \cdots + \binom{N}{r} + \cdots + \binom{N}{N},$$

$$N2^{N-1} = \binom{N}{1} + 2\binom{N}{2} + \cdots + r\binom{N}{r} + \cdots + N\binom{N}{N}.$$

Substracting (2.1) from the (2.2), we get

$$\binom{N}{2} + 2\binom{N}{3} + \cdots + (r-1)\binom{N}{r} + \cdots + (N-1)$$
$$= (N-2)2^{N-1} + 1.$$

□

An element $\gamma \in (\mathbb{Z}/p\mathbb{Z})^*$ is said to be a primitive root $\pmod p$ if γ is a generator of $(\mathbb{Z}/p\mathbb{Z})^*$. Once we know a primitive root $\pmod p$, all primitive roots $\pmod p$ are given by the set

$$\{\gamma^i : \gcd(i, p-1) = 1\}.$$

Consider a non-principal character $\chi : (\mathbb{Z}/p\mathbb{Z})^* \to \mu_{p-1}$, where μ_n denotes the subgroup of $\mathbb{C}^*$ of n-th roots of unity. Then one sees that $\chi(\gamma)$ is a primitive $(p-1)$-th root of unity if and only if γ is a primitive root $\pmod p$. Let η be a primitive $(p-1)$-th root of unity and assume that $\chi(\gamma) = \eta$. Since χ is a homomorphism, we have $\chi(\gamma^i) = \chi^i(\gamma) = \eta^i$. Hence by the above observation, it is clear that $\chi(\alpha) = \eta^i$ with $\gcd(i, p-1) = 1$ if and only if α is a primitive root $\pmod p$.

Let l be any non-negative integer. We define

$$\alpha_l(p-1) = \sum_{i=1,(i,p-1)=1}^{p-1} (\eta^i)^l.$$

Set $\chi_i = \chi^i$ for $1 \le i \le p-1$.

Let

$$f(x) = \frac{1}{2}\left(1 + \left(\frac{x}{p}\right)\right) \qquad \text{for all } x \in (\mathbb{Z}/p\mathbb{Z})^*$$

and

$$g(x) = \frac{1}{2}\left(1 - \left(\frac{x}{p}\right)\right) \quad \text{for all } x \in (\mathbb{Z}/p\mathbb{Z})^*,$$

where $\left(\frac{\cdot}{p}\right)$ is the Legendre symbol.

Clearly

$$f(x) = \begin{cases} 1, & \text{if } x \text{ is a quadratic residue} \pmod p \\ 0, & \text{otherwise} \end{cases}$$

and

$$g(x) = \begin{cases} 1, & \text{if } x \text{ is a quadratic nonresidue} \pmod p \\ 0, & \text{otherwise.} \end{cases}$$

Lemma 2.3. *We have*

$$\sum_{l=0}^{p-2} \alpha_l(p-1)\chi_l(x) = \begin{cases} p-1, & \text{if } x \text{ is a primitive root} \pmod p \\ 0, & \text{otherwise.} \end{cases}$$

Proof. See Lemma 2 in [13]. □

The following theorem was proved by Weil in [14].

Theorem 2.4. *For any integer l, $2 \leq l < p$ and for any non-principal characters $\chi_1, \ldots, \chi_l$ and distinct $a_1, \ldots, a_l \in \mathbb{Z}/p\mathbb{Z}$, we have*

$$\left|\sum_{x=1}^{p} \chi_1(x+a_1)\chi_2(x+a_2)\cdots\chi_l(x+a_l)\right| \leq (l-1)\sqrt{p}.$$

For a positive integer m, we denote $\omega(m)$ by the number of distinct prime factors of m.

Lemma 2.5. *We have*

$$\sum_{l=0}^{p-2} |\alpha_l(p-1)| = 2^{\omega(p-1)}\phi(p-1).$$

Proof. See [13]. □

Theorem 2.6. *For any prime p, let N_p denote the number of integers $1 < g < p-1$ which are primitive roots modulo p and coprime to $p-1$. Then*

$$N_p = \frac{\phi^2(p-1)}{p-1} + \frac{\phi(p-1)}{p-1}E_p,$$

where

$$|E_p| \leq 4^{\omega(p-1)}\sqrt{p}(\log p).$$

Proof. The proof can be found in [6]. □

3. Residues modulo p

Q1 Let $\mathtt{Q}(p, N)$ (respectively $\mathtt{N}(p, N)$) be the number of N consecutive quadratic residues (respectively nonresidues) modulo p in $(\mathbb{Z}/p\mathbb{Z})^*$. Then, using properties of $f(x)$ and $g(x)$, we see that

$$\mathtt{Q}(p, N) = \sum_{x=1}^{p-N} f(x)f(x+1)\cdots f(x+N-1)$$

and

$$\mathtt{N}(p, N) = \sum_{x=1}^{p-N} g(x)g(x+1)\cdots g(x+N-1).$$

We have the following technical lemma.

Lemma 3.1. *For any prime p and any positive integer $N \geq 3$, we have*

$$\left|\mathtt{Q}(p, N) - \frac{p}{2^N}\right| \leq \frac{\left((N-2)2^{N-1}+1\right)\sqrt{p}}{2^N}$$

and

$$\left|\mathtt{N}(p, N) - \frac{p}{2^N}\right| \leq \frac{\left((N-2)2^{N-1}+1\right)\sqrt{p}}{2^N}.$$

Proof. Consider

$$\begin{aligned}\mathtt{Q}(p, N) &= \sum_{x=1}^{p-N}\left\{\prod_{l=0}^{N-1} f(x+l)\right\} = \frac{1}{2^N}\sum_{x=1}^{p-N}\left\{\prod_{l=0}^{N-1}\left(1+\left(\frac{x+l}{p}\right)\right)\right\} \\ &\leq \frac{1}{2^N}\sum_{x=1}^{p}\left(1+\left(\frac{x}{p}\right)\right)\left(1+\left(\frac{x+1}{p}\right)\right)\cdots\left(1+\left(\frac{x+N-1}{p}\right)\right).\end{aligned}$$

Set $x_l = \left(\frac{x+l}{p}\right)$ for $l = 0, \ldots, N-1$. Since

$$\prod_{l=0}^{N-1}(1+x_l) = 1 + \sum_{l=0}^{N-1} x_l + \sum_{0\leq l_1<l_2\leq N-1} x_{l_1}x_{l_2} + \cdots + x_0x_1\cdots x_{N-1},$$

we have

$$\begin{aligned}\mathtt{Q}(p, N) \leq \frac{p}{2^N} + \frac{1}{2^N}&\left\{\sum_{l=0}^{N-1}\sum_{x=1}^{p}\left(\frac{x+l}{p}\right) + \sum_{0\leq l_1<l_2\leq N-1}\sum_{x=1}^{p}\left(\frac{(x+l_1)}{p}\right)\left(\frac{(x+l_2)}{p}\right)\right. \\ &\left. + \cdots + \sum_{x=1}^{p}\left(\frac{x}{p}\right)\left(\frac{x+1}{p}\right)\cdots\left(\frac{x+N-1}{p}\right)\right\}.\end{aligned}$$

By Theorem 2.4, we get

$$\left|\mathtt{Q}(p,N)-\frac{p}{2^N}\right| \le \frac{1}{2^N}\left\{\sum_{0\le l_1<l_2\le N-1}\sqrt{p}+\sum_{0\le l_1<l_2<l_3\le N-1}2\sqrt{p}+\cdots+(N-1)\sqrt{p}\right\}$$
$$=\frac{\sqrt{p}}{2^N}\left\{\binom{N}{2}+2\binom{N}{3}+\cdots+(N-1)\binom{N}{N}\right\}.$$

Now applying Lemma 2.2, we get

$$\left|\mathtt{Q}(p,N)-\frac{p}{2^N}\right| \le \frac{\left((N-2)2^{N-1}+1\right)\sqrt{p}}{2^N},$$

as desired.
Replacing the function f by g, we get the required estimate for $\mathtt{N}(p,N)$. □

Proof of Theorem 1.1. When $p=7$, we clearly see that $(1,2)$ is a consecutive pair of quadratic residue modulo 7. Assume that $p\ge 11$. If 10 is a quadratic residue modulo p, then we have $(9,10)$ as a consecutive pair of quadratic residues modulo p, otherwise as $10=2\times 5$, either 2 or 5 is a quadratic residue modulo p. Thus again either $(1,2)$ or $(4,5)$ serves as a consecutive pair of quadratic residues modulo p. Therefore, $\mathtt{Q}(p,2)>0$ for all primes $p\ge 7$.

Now when $p=5$, we see that $(2,3)$ is a consecutive pair of quadratic nonresidues and when $p=7$, $(5,6)$ serves the purpose. Assume that $p\ge 11$. Let $2\le a_1<a_2<\cdots<a_{\frac{p-1}{2}}\le p-1$ be all the quadratic nonresidues. If there are no consecutive pairs then $a_1\ge 2$, $a_2-a_1\ge 2$, and in general $a_{i+1}-a_i\ge 2$ for $1\le i\le \frac{p-3}{2}$, with at least one i such that $a_{i+1}-a_i>2$ as there exists a pair of consecutive quadratic residues. But this is impossible since we cannot fit $\frac{p-1}{2}$ numbers in $\{2,\ldots,p-1\}$ such that no two are consecutive and there are atleast two at a distance larger than 2 apart. This proves the theorem. □

Proof of Theorem 1.2. By Lemma 3.1, we have

$$-\mathtt{Q}(p,N)+\frac{p}{2^N}\le\left|\mathtt{Q}(p,N)-\frac{p}{2^N}\right|\le\frac{\left((N-2)2^{N-1}+1\right)\sqrt{p}}{2^N}.$$

Clearly $\mathtt{Q}(p,N)>0$ if

$$\frac{p}{2^N}>\frac{\left((N-2)2^{N-1}+1\right)\sqrt{p}}{2^N}\iff p>\left((N-2)2^{N-1}+1\right)\sqrt{p}.$$

Thus if $p>(N-2)^2 4^N$, then $\mathtt{Q}(p,N)>0$.

Similar arguments show that if $p>(N-2)^2 4^N$, then $\mathtt{N}(p,N)>0$. □

4. Primitive roots modulo p

Let $P(p,N)$ be the number of N consecutive primitive roots modulo p in $(\mathbb{Z}/p\mathbb{Z})^*$. We have the following lemma.

Lemma 4.1. *For any prime p and any positive integer N, we have*

$$\left| P(p, N) - p\left(\frac{\phi(p-1)}{p-1}\right)^N \right| \leq 2N\sqrt{p}2^{N\omega(p-1)}.$$

Proof. Replace $\beta_\ell(p-1)$ by $\alpha_\ell(p-1)$ and put $\phi(p-1)$ in place of k in Lemma 4 of [5] to get the required result. We shall omit the proof here. □

Proof of Theorem 1.3. Clearly, by Lemma 4.1, we have

$$p\left(\frac{\phi(p-1)}{p-1}\right)^N - P(p, N) \leq \left| P(p, N) - p\left(\frac{\phi(p-1)}{p-1}\right)^N \right| \leq 2N\sqrt{p}2^{N\omega(p-1)}.$$

Clearly $P(p, N) > 0$ if

$$p\left(\frac{\phi(p-1)}{p-1}\right)^N - 2N\sqrt{p}2^{N\omega(p-1)} > 0 \iff \sqrt{p}\left(\frac{\phi(p-1)}{p-1}\right)^N > 2N2^{N\omega(p-1)}.$$

This last inequality is satisfied if $\log p - 2N\log\frac{\phi(p-1)}{p-1} > 2(\log 2N) + 2N\omega(p-1)\log 2$. If $p > \mathrm{e}^{4N}$, then we see that $\frac{\log p}{2} > 2N\log\frac{\phi(p-1)}{p-1}$. Hence, if we prove that $\log p > 4(\log 2N) + 4N\omega(p-1)\log 2$, then it follows that $P(p, N) > 0$ for all $p > \mathrm{e}^{4N}$.

By Lemma 2, we have, $\omega(p-1) \leq (1.385)\dfrac{\log p}{\log\log p}$ holds for all prime $p \geq 5$. Thus for such primes the right-hand side of the above is bounded by

$$4\log(2N) + 4N \times 1.385\frac{\log p \log 2}{\log\log p}.$$

So, if we prove

$$\left(1 - \frac{4N \times 1.385\log 2}{\log\log p}\right)\log p > 4\log(2N),$$

we are done. Note that

$$\frac{4N \times 1.385\log 2}{\log\log p} < 1 \iff \log\log p > \log 2^{4N\times 1.385} \iff p > \exp(2^{5.54N}).$$

Also, we need

$$\log p > 4\log(2N) = \log(2^4 \cdot N^4) \iff p > 16N^4.$$

So if

$$p > \max\left\{\mathrm{e}^{2^{5.54N}}, 16N^4, \mathrm{e}^{4N}\right\} = \mathrm{e}^{2^{5.54N}}$$

we have $P(p, N) > 0$. □

Proof of Theorem 1.4. By Lemma 2.1(ii), we see that

$$4^{\omega(p-1)} \leq 4^{(1.385)\frac{\log p}{\log\log p}} < (6.83)^{\frac{\log p}{\log\log p}} = p^{\frac{\log 6.83}{\log\log p}}. \tag{4.3}$$

Let $\epsilon > 0$ be such that $0 < \epsilon < 1/2$. Then for all primes

$$p \geq \exp\exp\left(\frac{2\log 6.83}{1-2\epsilon}\right),$$

we have

$$4^{\omega(p-1)} < p^{\frac{1}{2}-\epsilon}, \tag{4.4}$$

which is an easy computation from (4.3) and (4.4). Therefore, $N_p \geq 1$ follows at once, if we prove that

$$\frac{\phi^2(p-1)}{p-1} > \frac{\phi(p-1)}{p-1} p^{1-\epsilon} \log p \text{ for all } p > \exp\exp\left(\frac{2\log 6.83}{1-2\epsilon}\right);$$

or if we prove $\phi(p-1) > p^{1-\epsilon}(\log p)$ for all primes p satisfying

$$p > \exp\exp\left(\frac{2\log 6.83}{1-2\epsilon}\right).$$

Note that

$$\frac{p-1}{\log(p-1)} > p^{1-\epsilon}\log p$$

is equivalent to

$$p > (\log(p-1)+1)^{2/\epsilon}.$$

Choose $\epsilon = 1/11$ and we check whether

$$\frac{p-1}{\log(p-1)} > p^{1-\epsilon}\log p$$

is true for this choice of ϵ. (Lemma 2.1(i) says that it is enough to check this inequality only to prove the theorem.) In fact, we get

$$\exp\exp\left(\frac{2\log 6.83}{1-2\epsilon}\right) = \exp\exp(\log(6.83)^{2.45}) = \exp((6.83)^{2.45}) < \mathrm{e}^{110.8}.$$

Choose primes $p > \mathrm{e}^{110.8}$ and we see that

$$\phi(p-1) > \frac{p-1}{\log(p-1)} > p^{10/11}\log p.$$

Therefore, $N_p \geq 1$ for all $p > \mathrm{e}^{110.8}$. This completes the proof. □

Acknowledgements

The first author would like to thank Harish Chandra Research Institute, Allahabad for financial support where he was working as a post doctoral fellow. The authors would like to thank the Institute of Mathematical Sciences, Chennai for the excellent facilities provided during their visit as a part of the special year in Number Theory where this work was finalized.

References

[1] Brauer A, Űber Sequenzen von Potenzresten, Sitzungsberichte der Preubischen Akademie der Wissenschaften (1928) pp. 9–16

[2] Carlitz L, Sets of primitive roots, *Compositio Math.* **13** (1956) 65–70

[3] Gowers W T, A new proof of Szemerédi's theorem, *Geom. Funct. Anal.* **11(3)** (2001) 465–588

[4] Gun S, Ramakrishnan B, Sahu B and Thangadurai R, Distribution of quadratic non-residues which are not primitive roots, *Math. Bohem.* **130(4)** (2005) 387–396

[5] Gun S, Luca F, Rath P, Sahu B and Thangadurai R, Distribution of residues modulo p, *Acta Arith.* **129(4)** (2007) 325–333

[6] Hausman M, Primitive roots satisfying a coprime condition, *Am. Math. Monthly* **83** (1976) 720–723

[7] Luca F, Shparlinski I E and Thangadurai R, Quadratic non-residue verses primitive roots modulo p, *J. Ramanujan Math. Soc.* **23(1)** (2008) 97–104

[8] Luca F and Thangadurai R, Distribution of Resodues Modulo p – II, to appear in the Ramanujan Mathematical Society Lecture Notes Series (2011) Q2

Q3 [9] Moser L, On the equation $\phi(n) = \pi(n)$, *Pi Mu Epsilon J.* (1951) 101–110

Q4 [10] Problems and Solutions, Problem E-2488, this MONTHLY, **81** (1974) 776

[11] Sándor J, Mitrinović D S and Crstici B, Handbook on Number Theory I (The Netherlands: Springer) Q5

[12] Szalay M, On the distribution of the primitive roots mod p (in Hungarian), *Mat. Lapok* **21** (1970) 357–362

[13] Szalay M, On the distribution of the primitive roots of a prime, *J. Number Theory* **7** (1975) 183–188

[14] Weil A, On the Riemann hypothesis, *Proc. Nat. Acad. Sci. USA* **27** (1941) 345–347

AUTHOR QUERIES

AUTHOR PLEASE ANSWER ALL QUERIES.

Q1. Please check output for ‘Q’ and ‘N’ if correct.
Q2. Please provide details for reference item [8] if any.
Q3. Please provide volume number for reference item [9].
Q4. Please check reference item [10] if captured correctly.
Q5. Please provide year of publication for reference item [11].