Proceedings of the Jangjeon Mathematical Society
25 (2022), No. 3, pp. 355 – 357

www.jangjeon.or.kr
http://dx.doi.org/10.17777/pjms2022.25.3.355

A NOTE ON THE LEAST NONRESIDUE MODULO PRIME $p \equiv 7 \pmod 8$

SHIVARAJKUMAR, CH. SRIKANTH

Abstract. In 2008, Andrew Granville proved that, Vinogradov's conjecture on the least nonresidue modulo primes p with $p \equiv 3 \pmod 4$ is true if every interval of length p near to p contains a $p^\epsilon-$smooth integer for all sufficiently large p. In this short note, we prove that it is enough to find a $p^\epsilon-$smooth integer in the interval $[\frac{p-1}{2} - \lfloor \frac{p^\epsilon}{2} \rfloor, \ \frac{p-1}{2}]$. Further, when $\epsilon = 1/2$, we provide a new proof of the Vinogradov's conjecture.

2010 Mathematics Subject Classification. 11A07, 11B75.

Keywords. Quadratic residues, least nonresidue, smooth integer

1. Introduction

Let p be a prime. An integer q is called a quadratic residue modulo p, if it is congruent to a square modulo p. That is, if there exists an integer x such that,

$$x^2 \equiv q \pmod p.$$

Otherwise, q is called a nonresidue modulo p.

Let $n(p)$ denote the least positive integer that is not a quadratic residue modulo p. The Polya-Vinogradov bound on character sums implies that $n(p) \ll \sqrt{p} \log p$ and then Vinogradov [8] reduced this bound to

$$n(p) \ll p^{\frac{1}{\sqrt{2e}}} \log^2 p$$

for all primes p and made the following conjecture.

Vinogradov's Conjecture. For any fixed real $\epsilon > 0$, we have $n(p) \ll_\epsilon p^\epsilon$.

In 1942, Linnik [5] proved that, this conjecture follows from the Generalised Riemann Hypothesis (GRH). In 1952, Ankeny [1] improved the bound further to $n(p) \ll \log^2 p$ under the same hypothesis. However the conjecture remains open unconditionally.

In 1957, Burgess [2] proved that Vinogradov's conjecture is true for any $\epsilon > \frac{1}{4\sqrt{e}}$, without assuming the validity of GRH. Till today this result remains to be the best known bound.

Smoothness property. A positive integer x is called $y-$*smooth* if none of its prime factors is greater than y.

In 2008, Andrew Granville [3] showed that Vinogradov's conjecture is true for primes $p \equiv 3 \pmod 4$, if "smoothness in short intervals" conjecture is true. The "smoothness in short intervals" conjecture predicts that every interval of length x^ϵ

close to x contains an $x^{\epsilon}-$ smooth integer for all large enough x. Andrew Granville [3] mentioned that, in some situations there are sharp estimates in wide ranges, and yet in other seemingly tractable situations, there does seem to be serious difficulty in extending the smoothness range of what is known. In particular, it is intriguingly difficult to prove that there are smooth numbers in all intervals of length $\sqrt{x}$, close to x. However, he remains hopeful that "smoothness in short intervals" problem might succumb to a clever combinatorial argument, rather than sophisticated technique.

In this note, we see that it is enough to have "smoothness in short intervals" property hold for certain intervals in order for Vinogradov's conjecture to be true for primes $p \equiv 3 \pmod 4$. Precisely, we show that Vinogradov's conjecture is true if there exists a $p^{\epsilon}-$ smooth integer in the interval $[\frac{p-1}{2} - \lfloor \frac{p^{\epsilon}}{2} \rfloor, \ \frac{p-1}{2}]$. Further, our arguments show that Vinogradov's conjecture is true for $\epsilon = \frac{1}{2}$ independent of the smoothness property, and thereby deduce that the interval $[\frac{p-1}{2} - \lfloor \frac{\sqrt{p}}{2} \rfloor, \ \frac{p-1}{2}]$ contains a $\sqrt{p}$-smooth integer for primes $p \equiv 3 \pmod 4$. We note that proofs [4, 6] exist for the Vinogradov's conjecture for $\epsilon = 1/2$. Our present proof is interesting as it shows a connection between least nonresidue modulo prime and the smoothness property.

2. Results

In this section, we prove that, to prove Vinogradov's conjecture for $p \equiv 3 \pmod 4$, it is enough to find the $p^{\epsilon}-$smooth integer in the interval $[\frac{p-1}{2} - \lfloor \frac{p^{\epsilon}}{2} \rfloor, \ \frac{p-1}{2}]$.

Note 2.1. *We know that, when $p \equiv 3 \pmod 8$, 2 is a nonresidue mod p. Hence $n(p) = 2$. Therefore, it is enough to find $p^{\epsilon}-$smooth intger in the interval $[\frac{p-1}{2} - \lfloor \frac{p^{\epsilon}}{2} \rfloor, \ \frac{p-1}{2}]$ for primes $p \equiv 7 \pmod 8$.*

Lemma 2.2. *For $p \equiv 7 \pmod 8$, if $n(p)$ is the first nonresidue, then all the integers in $[\frac{p-1}{2} - \frac{n(p)-3}{2}, \frac{p-1}{2}]$ are nonresidues.*

Proof. For a given prime $p \equiv 7 \pmod 8$, we know that $\{1, 2, 3, ..., n(p) - 1\}$ are all quadratic residues and $n(p)$ is the first nonresidue. Since 2 is a quadratic residue, $\frac{p-1}{2}$ is a nonresidue. Let X denote the set of all odd integers from 1 to $n(p) - 1$. Multiply $\frac{p-1}{2}$ with all the elements of X, we get consecutive integers $\frac{p-1}{2} - \frac{n(p)-3}{2}$, $\frac{p-1}{2} - \frac{n(p)-5}{2}$, ,..., $\frac{p-1}{2} - 1$, $\frac{p-1}{2}$. It is easy to see that all these integers are nonresidues because the product of a residue and a nonresidue is nonresidue. □

As an immediate consequence, we prove the following.

Theorem 2.3. *For every prime $p \equiv 7 \pmod 8$, $n_p < \sqrt{p-1} + 1$.*

Proof. If we multiply $\frac{p-1}{2} - \frac{n(p)-3}{2}$ with all the elements of X (defined in Lemma 2.1), we get an arithmetic progression of nonresidues,

$$\frac{p-1}{2} - \frac{n(p)-3}{2}(n(p)-1), \frac{p-1}{2} - \frac{n(p)-3}{2}(n(p)-2), ..., \frac{p-1}{2} - \frac{n(p)-3}{2}$$

with common difference $n(p) - 1$. But,

$$[\frac{p-1}{2} - \frac{n(p)-3}{2}]((n(p)-1) > n(p) - 1.$$

This implies, $\frac{p-1}{2} - (\frac{n(p)-3}{2}) - (\frac{n(p)-3}{2})(n(p)-1) > (n(p)-1)$.
Therefore, $\frac{p-1}{2} > (n(p)-1) + (\frac{n(p)-3}{2})(n(p)-1)$.
On simplification, we get $p-1 > (n(p)-1)(n(p)-1)$.
Therefore, $n(p) < \sqrt{p-1}+1$. □

Theorem 2.3 proves that Vinogradov's conjecture is true for primes $p \equiv 7 \pmod 8$ when $\epsilon = 1/2$. From this result, one can see that there exists a $\sqrt{p}$-smooth integer in the interval $[\frac{p-1}{2} - [\frac{\sqrt{p}}{2}], \frac{p-1}{2}]$ for primes $p \equiv 7 \pmod 8$.

As a corollary to the above lemma, we have the following.

Corollary 2.4. *Let ϵ be any positive real number. For prime $p \equiv 7 \pmod 8$, if there exists a p^ϵ-smooth integer in an interval $[\frac{p-1}{2} - \lfloor \frac{p^\epsilon}{2} \rfloor, \frac{p-1}{2}]$ then $n(p) < p^\epsilon$.*

Proof. Suppose that there is an integer say k in the interval $[\frac{p-1}{2} - \frac{n(p)-3}{2}, \frac{p-1}{2}]$, which is $p^\epsilon-$smooth. From the above lemma, the result follows. □

Corollary 2.4 establishes a connection between the magnitude of $n(p)$ and smoothness property in a specific interval for $\epsilon < 1/2$. From this result, one can see that if "smoothness in short intervals" property holds for certain intervals, then Vinogradov's conjecture is true for $\epsilon < 1/2$ and for primes $p \equiv 7 \pmod 8$.

Note 2.5. *From Lemma 2.1, we have seen that, all integers in the interval $[\frac{p-1}{2} - \frac{n(p)-3}{2}, \frac{p-1}{2}]$ are nonresidues. We know that, $n(p)$ is a prime number. Thus, every integer in the interval $[\frac{p-1}{2} - \frac{n(p)-3}{2}, \frac{p-1}{2}]$ should be k-smooth, where $k \geq n(p)$. With this condition, we have totally $\lfloor n(p)/2 \rfloor$ consecutive integers which should be k-smooth. This suggests that $n(p)$ can not be very large quantity, for example p^ϵ as suggested by Vinogradov's conjecture. But one requires a formal argument to prove it rigorously.*

Acknowledgement. We would like to thank referees for their valuable comments and suggestions to improve the overall presentation of the paper.

References

[1] N. C. Ankeny, *The least quadratic non residue*, Ann. of Math., **55(2)** (1952) 65-72.
[2] D. A. Burgess, *The distribution of quadratic residues and non-residues*, Mathematika, **4** (1957) 106-112.
[3] A. Granville, *Smooth numbers: computational number theory and beyond*, Algorithmic number theory, **44**, (2008) 267-323.
[4] P. Hummel, *On consecutive quadratic non-residues: a conjecture of Issai Schur*, Journal of Number Theory **103** (2003) 257-266.
[5] U. V. Linnik, *A remark on the least quadratic non-residue*, C. R.(Doklady) Acad. Sci. URSS (N.S.), **36**, (1942) 119-120.
[6] Shivarajkumar, *Beyond Schur's conjecture*, Amer. Math. Monthly, **123**, (2016) 64-67.
[7] I. Vinogradov, *Űber die Verteilung der quadratischen Reste und Nichtreste*, J. Sot. Phys. Math. Univ. Permi. **2** (1919) 1-14.
[8] I. Vinogradov, *On a general theorem concerning the distribution of the residuesand nonresidues of powers*, Trans. American Math. Soc., **29** (1927), 209-217.

The National Institute of Engineering, Mysuru, Vijna Research Labs, Bengaluru
Email address: shivarajmacs@nie.ac.in, sricheru1214@gmail.com