DEMONSTRATIO MATHEMATICA
Vol. XXVIII No 3 1995

Stefan Chaładus

AN APPLICATION OF NAGELL'S ESTIMATE OF THE LEAST ODD QUADRATIC NONRESIDUE

Let p be an odd prime, $A_p = \{1, 2, \ldots, p-1\} \subset N$ — the multiplicative group mod p, R_p — the subset of quadratic residues mod p and N_p — the subset of quadratic nonresidues. Let us denote for an $a \in A_p$ by $\overline{a}$ the inverse element of A_p.

The subset

$$L_p = \{a \in A_p : \; a \equiv \overline{a} \bmod 2\}$$

has been considered by D. H. Lehmer [1] who asked: what can be said about L_p?

G. Terjanian (working on another problem) has proposed three conjectures [4]:

(1) $L_p \subset R_p$ if and only if $p = 5, 13$ or 29,
(2) $R_p \subset L_p$ if and only if $p = 3, 5, 7$ or 13,
(3) $N_p \subset L_p$ if and only if $p = 3$ or 7,

and has proved them, among other partial results, in the case $p \equiv 3 \bmod 4$.

Let us observe that if $L_p \cap N_p$ or $R_p \setminus L_p$ or $N_p \setminus L_p$ are non-empty subsets of A_p, then (1), (2), (3) are true respectively. Further on we shall indicate for each of these subsets an element that belongs to it. The proofs are elementary but require discrimination of several cases with respect to a form of p.

I. Z. Ruzsa and A. Schinzel [4] have proved that each of the sets $L_p \cap N_p$, $L_p \cap R_p$, $R_p \setminus L_p$ and $N_p \setminus L_p$ has $\frac{1}{4}p + O(\sqrt{p}(\log p)^2)$ elemetns. This implies Terjanian's conjectures but only for p large enough.

To end this introduction we remind that

(4) if $p \equiv 1 \bmod 4$, then $a \in R_p \Leftrightarrow p - a \in R_p$,
(5) if $p \equiv 3 \bmod 4$, then $a \in R_p \Leftrightarrow p - a \in N_p$,
(6) $2 \in R_p \Leftrightarrow p \equiv \pm 1 \bmod 8$,

and as a consequence of the quadratic reciprocity law

(7) if $p \equiv 1 \bmod 4$, then $3 \in R_p \Leftrightarrow p \equiv 1 \bmod 3$,

(8) if $p \equiv 3 \bmod 4$, then $3 \in R_p \Leftrightarrow p \equiv 2 \bmod 3$.

The proofs of conjectures (1), (2), (3) are based on several lemmas.

LEMMA 1. *If $p > 7$ and either $L_p \subset R_p$ or $R_p \subset L_p$ or $N_p \subset L_p$ we have $p \equiv 1 \bmod 4$.*

Proof. If $L_p \subset R_p$ we have $p - 1 \in R_p$, hence $p \equiv 1 \bmod 4$.

Let
$$p + 1 = 2^\alpha \cdot s, \qquad 2 \nmid s.$$

If $s > 1$ then $s \notin L_p$ and $p - s \notin L_p$, consequently the alternative $R_p \subset L_p$ or $N_p \subset L_p$ implies that $p \equiv 1 \bmod 4$.

If $s = 1$ then $\alpha > 3$ is prime and so odd, hence $p \equiv 1 \bmod 3$.

We have
$$\frac{p+8}{3} \cdot 3 \cdot 2^{\alpha-3} \equiv 1 \bmod p,$$
hence $a = (p + 8)/3 \notin L_p$ and $p - a \notin L_p$, consequently the alternative $R_p \subset L_p$ or $N_p \subset L_p$ implies that $p \equiv 1 \bmod 4$.

Therefore, we may assume in further arguments that $p \equiv 1 \bmod 4$. In the proofs of Lemma 2 and 4 the following property is used:

If $p \equiv 1 \bmod 24$ then there exists a quadratic nonresidue a mod p such that

(9) $a < p/2, \qquad 3 \mid a \quad \text{and} \quad a \equiv 3 \bmod 4.$

Since $p \equiv 1 \bmod 24$ implies that 2 and 3 are both quadratic residues mod p, it is easy to see that (9) is satisfied if there exists a quadratic nonresidue $a < p/18$, what happens to be true for all $p > 73$, by a theorem of Nagell [2], [3]. The direct check shows however that (9) is satisfied also for $p = 73$ with $a = 15$.

LEMMA 2. *$L_p \subset R_p$ if and only if $p = 5, 13$ or 29.*

Proof. a1) $p \equiv 5 \bmod 16$. We have
$$8 \cdot \frac{3p+1}{8} \equiv 1 \bmod p,$$
hence $8 \in L_p \cap N_p$, provided $p > 5$.

a2) $p \equiv 13 \bmod 16$. If $p = 48k + 13$, $k = 0, 1, 2, \ldots$, then
$$24 \cdot \frac{11p+1}{24} \equiv 1 \bmod p,$$
hence $24 \in L_p \cap N_p$, provided $p > 13$. If $p = 48k + 29$, $k = 0, 1, 2 \ldots$, then $2p - 16 = 3(32k + 14)$, hence $32k + 14$ is a quadratic nonresidue mod p. We

have

$$48(43k+26) \equiv 1 \bmod p \quad \text{and} \quad (32k+14)(45k+27) \equiv 1 \bmod p.$$

Therefore $32k+14 \in L_p \cap N_p$ if k is odd or $48 \in L_p \cap N_p$ if $k > 0$ is even.

b) $p \equiv 1 \bmod 8$. If $p = 24k+17$, $k = 0,1,2,\ldots$, then

$$12 \cdot \frac{7p+1}{12} \equiv 1 \bmod p,$$

hence $12 \in L_p \cap N_p$. Finally, let $p = 24k+1$, $k = 1,2,\ldots$, let $a \in A_p$ satisfy (9) and let $b = \overline{a}$. Obviously, if $2 \nmid b$ then $a \in L_p \cap N_p$. If $4 \mid b$ then

$$2a \cdot \frac{b}{2} \equiv 1 \bmod p,$$

hence $2a \in L_p \cap N_p$. Let then $b \equiv 2 \bmod 4$.

i) If $b < p/2$ then

$$\frac{p+a}{2} \cdot 2b \equiv 1 \bmod p,$$

hence $2b \in L_p \cap N_p$.

ii) If $p/3 < b < 2p/3$ then

$$\frac{a}{3} \cdot (3b-p) \equiv 1 \bmod p,$$

hence $a/3 \in L_p \cap N_p$.

iii) If $b > 2p/3$ then

$$\frac{2a}{3} \cdot \frac{3b-2p}{2} \equiv 1 \bmod p,$$

hence $2a/3 \in L_p \cap N_p$.

LEMMA 3. *$R_p \subset L_p$ if and only if $p = 3, 5, 7$ or 13.*

Proof. a) $p \equiv 1 \bmod 8$. We have

$$2 \cdot \frac{p+1}{2} \equiv 1 \bmod p.$$

hence $2 \in R_p \setminus L_p$.

b) $p \equiv 5 \bmod 8$. If $p = 24k+5$, $k = 0,1,2,\ldots$, then

$$6 \cdot \frac{p+1}{6} \equiv 1 \bmod p,$$

hence $6 \in R_p \setminus L_p$, provided $p > 5$. Let us divide the complete case $p = 24k+13$, $k = 0,1,2,\ldots$, into subcases

b1) $p = 72k+13$,
b2) $p = 72k+37$,
b3) $p = 72k+61$.

b1.1) If $p = 144k + 13$, $k = 0, 1, 2, \ldots$, then $p - 16 = 3(48k - 1)$ and $4p - 16 = 9(64k + 4)$, hence $48k - 1$ and $64k + 4$ are both quadratic residues mod p. We have

(10) $(64k + 4)(117k + 10) \equiv 1 \bmod p$ and $(48k - 1)(135k + 12) \equiv 1 \bmod p$.

Therefore (10) implies that $64k+4 \in R_p \setminus L_p$ if k is odd or $48k-1 \in R_p \setminus L_p$ if $k > 0$ is even.

b1.2) If $p = 144k + 85$, $k = 1, 2, \ldots$, then we have

$$48(105k + 62) \equiv 1 \bmod p \quad \text{and} \quad 144(83k + 49) \equiv 1 \bmod p,$$

hence $48 \in R_p \setminus L_p$ if k is odd or $144 \in R_p \setminus L_p$ if k is even.

b2) $p = 72k + 37$, $k = 0, 1, 2, \ldots$. Then $p - 1 = 9(8k + 4)$, hence $8k + 4$ and so $32k + 16$ is a quadratic residue mod p. We have

$$(32k + 16)(18k + 7) \equiv 1 \bmod p,$$

hence $32k + 16 \in R_p \setminus L_p$.

b3) $p = 72k + 61$, $k = 0, 1, 2, \ldots$. We have

$$9 \cdot \frac{5p + 1}{9} \equiv 1 \bmod p,$$

hence $9 \in R_p \setminus L_p$.

LEMMA 4. *$N_p \subset L_p$ if and only if $p = 3$ or 7.*

Proof. a) $p \equiv 5 \bmod 8$. We have

$$2 \cdot \frac{p + 1}{2} \equiv 1 \bmod p,$$

hence $2 \in N_p \setminus L_p$.

b) $p \equiv 1 \bmod 8$. If $p = 24k + 17$, $k = 0, 1, 2, \ldots$, then

$$3 \cdot \frac{p + 1}{3} \equiv 1 \bmod p,$$

hence $3 \in N_p \setminus L_p$. Finally, let $p = 24k + 1$, $k = 1, 2, \ldots$, let $a \in A_p$ satisfy (9) and let $b = \overline{a}$. Obviously, if $2 \mid b$ then $a \in N_p \setminus L_p$. If $b \equiv 1 \bmod 4$, then

$$2a \cdot \frac{p + b}{2} \equiv 1 \bmod p,$$

hence $2a \in N_p \setminus L_p$. Let then $b \equiv 3 \bmod 4$.

i) If $b > p/2$ then

$$\frac{p - a}{2} \cdot 2(p - b) \equiv 1 \bmod p,$$

hence $(p - a)/2 \in N_p \setminus L_p$.

ii) If $p/3 < b < 2p/3$ then

$$\frac{a}{3}(3b - p) \equiv 1 \bmod p,$$

hence $a/3 \in N_p \setminus L_p$.

iii) If $b < p/3$ then

$$\frac{2a}{3} \cdot \frac{p + 3b}{2} \equiv 1 \bmod p,$$

hence $2a/3 \in N_p \setminus L_p$.

Acknowledgement. The author wishes to express his thanks to Professor Andrzej Schinzel for suggesting the problem, pointing out mistakes in proofs of Lemma 2 and for his help in the preparation of this article.

References

[1] R. K. Guy, *Unsolved problems in number theory*, (Problem F12 on page 139), Springer-Verlag, 1981.

[2] T. Nagell, *Sur les restes et non-restes quadratiques suivant un module premier*, Ark. Mat. 1(1950), 185–193.

[3] T. Nagell, *Sur le plus petit non-reste quadratique impair*, Ark. Mat. 1(1951), 573–578.

[4] I. Z. Ruzsa and A. Schinzel, *An application of Kloosterman sums*, to appear.

INSTITUTE OF MATHEMATICS
PEDAGOGICAL UNIVERSITY
M. Konopnickiej 21
25-406 KIELCE, POLAND

Received November 4, 1993.