MATH. SCAND. 2 (1954), 187–192

ÜBER DEN KLEINSTEN POSITIVEN QUADRATISCHEN NICHTREST

BENGT STOLT

1. Es sei p eine ungerade Primzahl. Mit $\psi^\star(p;\,2) = \psi^\star$ bezeichnen wir die kleinste ungerade positive ganze Zahl, die quadratischer Nichtrest modulo p ist. Es ist klar, dass $\psi^\star$ stets eine Primzahl ist.

Das Problem, eine obere Grenze für $\psi^\star$ zu finden, wurde zum erstenmal im Jahre 1923 von T. Nagell [1, pp. 7–10] behandelt. Mit sehr einfachen Methoden zeigte er, dass für alle Primzahlen p die Ungleichung

$$\psi^\star < 2p^{\frac{1}{2}} + 1$$

gilt. In späteren Arbeiten [2; 3] hat er diese Ungleichung verbessert und mittels einer neuen Methode die folgenden Ungleichungen bewiesen:

$$\begin{aligned}
&\psi^\star \leqq [\tfrac{1}{2}(p+1)]^{\frac{1}{2}}, && p \equiv 1 \pmod 8, && p \neq 17\,,\\
&\psi^\star \leqq (p-6)^{\frac{1}{2}}, && p \equiv -1 \pmod 8, && p \neq 7,\,23\,,\\
&\psi^\star \leqq 2+(p-4)^{\frac{1}{2}}, && p \equiv 5 \pmod 8\,.
\end{aligned}$$

In einer soeben publizierten Arbeit hat L. Rédei [4] gezeigt, dass die Ungleichung

$$\psi^\star < p^{\frac{1}{2}}, \qquad p \equiv \pm 3 \pmod 8\,,$$

mit Ausnahme der Werte $p = 3,\,5,\,11,\,13,\,59,\,109,\,131$ gilt. Der Beweis wird durch eine Verfeinerung einer von Nagell [1, pp. 7–10] benutzten Methode geführt.

Es ist aber möglich, das Resultat von Rédei zu verschärfen. In der vorliegenden Note werden wir die Ungleichung

$$\psi^\star < (\tfrac{1}{2}p)^{\frac{1}{2}}, \qquad p \equiv 5 \pmod 8, \quad p \neq 5,\,13,\,37,\,61,\,109\,,$$

herleiten. Aus dem Beweise geht hervor, dass man auch in den Fällen $p \equiv -1 \pmod 8$ und $p \equiv 3 \pmod 8$ ähnliche Verschärfungen beweisen kann.

Eingegangen am 4. Juni 1954.

Bedingungen für e	Die ganzen Zahlen a und b	Der Wert von $b-a$	Ausnahmewerte für e
$3\mid e$, $e \equiv 0 \pmod 8$, $e \geqq 4$	$a = \frac{1}{8}[p-(2e+3)(e-1)]$ $b = \frac{1}{8}[p-(2e+9)(e-3)]$	$b-a = -\frac{1}{4}e+3$	
$3\mid e$, $e \equiv 2 \pmod 8$, $e \geqq 4$	$a = \frac{1}{8}[p-(2e-3)(e+3)]$ $b = \frac{1}{8}[p-(2e+9)(e-1)]$	$b-a = -\frac{1}{2}e$	
$3\mid e$, $e \equiv 4 \pmod 8$, $e \geqq 71$	$a = \frac{1}{8}[p-(2e-15)(e+9)]$ $b = \frac{1}{8}[p-(2e+33)(e-15)]$	$b-a = 45$	12, 36, 60
$3\mid e$, $e \equiv 6 \pmod 8$, $e \geqq 33$	$a = \frac{1}{8}[p-(2e+27)(e-11)]$ $b = \frac{1}{8}[p-(2e+15)(e-7)]$	$b-a = \frac{1}{2}e-24$	6, 30
$3\mid e+1$, $e \equiv 0 \pmod 8$, $e \geqq 98$	$a = \frac{1}{8}[p-(2e+5)(e+1)]$ $b = \frac{1}{8}[p-(2e-43)(e+25)]$	$b-a = 135$	8, 32, 56, 80
$3\mid e+1$, $e \equiv 2 \pmod 8$, $e \geqq 51$	$a = \frac{1}{8}[p-(2e-7)(e+7)]$ $b = \frac{1}{8}[p-(2e+23)(e-11)]$	$b-a = \frac{1}{4}(3e+2)+25$	26, 50
$3\mid e+1$, $e \equiv 4 \pmod 8$, $e \geqq 17$	$a = \frac{1}{8}[p-(2e+5)(e-3)]$ $b = \frac{1}{8}[p-(2e+17)(e-7)]$	$b-a = \frac{1}{2}e-13$	
$3\mid e+1$, $e \equiv 6 \pmod 8$, $e \geqq 4$	$a = \frac{1}{8}[p-(2e-1)(e+1)]$ $b = \frac{1}{8}[p-(2e+5)(e-1)]$	$b-a = \frac{1}{4}(e-2)$	
$3\mid e-1$, $e \equiv 0 \pmod 8$, $e \geqq 37$	$a = \frac{1}{8}[p-(2e+13)(e-7)]$ $b = \frac{1}{8}[p-(2e+7)(e-5)]$	$b-a = \frac{1}{4}e-7$	16
$3\mid e-1$, $e \equiv 2 \pmod 8$, $e \geqq 9$	$a = \frac{1}{8}[p-(2e+13)(e-5)]$ $b = \frac{1}{8}[p-(2e+7)(e-3)]$	$b-a = \frac{1}{4}(e-2)-5$	
$3\mid e-1$, $e \equiv 4 \pmod 8$, $e \geqq 4$	$a = \frac{1}{8}[p-(2e+13)(e-3)]$ $b = \frac{1}{8}[p-(2e+7)(e-1)]$	$b-a = \frac{1}{4}e-4$	
$3\mid e-1$, $e \equiv 6 \pmod 8$, $e \geqq 81$	$a = \frac{1}{8}[p-(2e-5)(e+5)]$ $b = \frac{1}{8}[p-(2e+43)(e-19)]$	$b-a = 199$	22, 46, 70
$3\mid e$, $e \equiv 1 \pmod 8$, $e \geqq 5$	$a = \frac{1}{8}[p-(2e+9)(e-2)]$ $b = \frac{1}{8}[p-(2e+15)(e-4)]$	$b-a = \frac{1}{4}(e-1)-5$	
$3\mid e$, $e \equiv 3 \pmod 8$, $e \geqq 101$	$a = \frac{1}{8}[p-(2e-9)(e+6)]$ $b = \frac{1}{8}[p-(2e+39)(e-18)]$	$b-a = 81$	27, 51, 75, 99
$3\mid e$, $e \equiv 5 \pmod 8$, $e \geqq 49$	$a = \frac{1}{8}[p-(2e-21)(e+12)]$ $b = \frac{1}{8}[p-(2e+27)(e-12)]$	$b-a = 9$	21, 45
$3\mid e$, $e \equiv 7 \pmod 8$, $e \geqq 13$	$a = \frac{1}{8}[p-(2e+15)(e-6)]$ $b = \frac{1}{8}[p-(2e+3)(e-2)]$	$b-a = \frac{1}{2}(e-1)-10$	
$3\mid e+1$, $e \equiv 1 \pmod 8$, $e \geqq 38$	$a = \frac{1}{8}[p-(2e-19)(e+10)]$ $b = \frac{1}{8}[p-(2e+5)(e-4)]$	$b-a = \frac{1}{4}(e-1)-21$	17
$3\mid e+1$, $e \equiv 3 \pmod 8$, $e \geqq 22$	$a = \frac{1}{8}[p-(2e-13)(e+10)]$ $b = \frac{1}{8}[p-(2e+11)(e-6)]$	$b-a = e-8$	11
$3\mid e+1$, $e \equiv 5 \pmod 8$, $e \geqq 6$	$a = \frac{1}{8}[p-(2e+11)(e-4)]$ $b = \frac{1}{8}[p-(2e+5)(e-2)]$	$b-a = \frac{1}{4}(e-1)-4$	5
$3\mid e+1$, $e \equiv 7 \pmod 8$, $e \geqq 4$	$a = \frac{1}{8}[p-(2e+11)(e-2)]$ $b = \frac{1}{8}[p-(2e+5)e]$	$b-a = \frac{1}{4}(e-3)-2$	
$3\mid e-1$, $e \equiv 1 \pmod 8$, $e \geqq 10$	$a = \frac{1}{8}[p-(2e+7)(e-4)]$ $b = \frac{1}{8}[p-(2e+1)(e-2)]$	$b-a = \frac{1}{4}(e-1)-3$	
$3\mid e-1$, $e \equiv 3 \pmod 8$, $e \geqq 10$	$a = \frac{1}{8}[p-(2e+19)(e-6)]$ $b = \frac{1}{8}[p-(2e+7)(e-2)]$	$b-a = \frac{1}{2}(e-1)-12$	
$3\mid e-1$, $e \equiv 5 \pmod 8$, $e \geqq 4$	$a = \frac{1}{8}[p-(2e+7)e]$ $b = \frac{1}{8}[p-(2e+1)(e+2)]$	$b-a = \frac{1}{4}(e-1)$	
$3\mid e-1$, $e \equiv 7 \pmod 8$, $e \geqq 66$	$a = \frac{1}{8}[p-(2e-11)(e+8)]$ $b = \frac{1}{8}[p-(2e+37)(e-16)]$	$b-a = 63$	7, 31, 55

2. Wir wollen nun den folgenden Satz beweisen.

SATZ. *Wenn p eine Primzahl $\equiv 5 \pmod 8$ ist, besteht die Ungleichung*

$$\psi^* < (\tfrac{1}{2}p)^{\frac{1}{2}}$$

abgesehen von den folgenden Werten von p:

$$5,\ 13,\ 37,\ 61,\ 109\ .$$

BEWEIS. Bezeichnet e die grösste natürliche Zahl $< (\frac{1}{2}p)^{\frac{1}{2}}$, so gilt

$$0 < p - 2e^2 < 4e + 2\ .$$

Wir wollen annehmen, dass

$$e \geqq 5$$

ist. Denn für $e < 5$ ist $p = 29$ die einzige Primzahl, für welche der Satz gilt. Die übrigen Primzahlen $p = 5$, 13 und 37 sind Ausnahmewerte, was man leicht nachprüfen kann.

Wir werden zeigen, dass ganze positive ungerade Zahlen u_1, u_1', v, v', alle $\leqq e$, existieren, derart dass

$$0 < |a| \leqq e, \qquad 0 < |b| \leqq e, \qquad a-b \text{ ungerade},$$

wobei hier

$$a = \tfrac{1}{8}(p - uv), \qquad b = \tfrac{1}{8}(p - u'v'), \qquad u = 3u_1, \qquad u' = 3u_1'\ .$$

Da -1 quadratischer Rest mod. p ist, so dass $p-uv$ und $p-u'v'$ quadratische Reste oder Nichreste sind, je nachdem $-uv$ und $-u'v'$ Reste bzw. Nichtreste sind, während 2 quadratischer Nichtrest ist, leuchtet ein, dass sowohl eine der Zahlen a, 3, u_1, v als auch mindestens eine der Zahlen b, 3, u_1', v' quadratischer Nichtrest sein muss. Hieraus folgt offenbar, dass unter den Zahlen

$$1,\ 3,\ 5,\ \ldots \leqq e$$

mindestens ein Nichtrest auftritt.

Die Existenz solcher Zahlen u_1, u_1', v, v', a, b geht aus der vorstehenden Tabelle hervor. Es ist nötig, 24 Fälle zu unterscheiden.

Schliesslich betrachten wir diejenigen Primzahlen, die den Ausnahmewerten von e entsprechen. Zuerst betrachten wir eine Primzahl $p \equiv 13 \pmod{40}$ oder $p \equiv 37 \pmod{40}$. Dann ist leicht einzusehen, dass 5 quadratischer Nichtrest modulo p ist. Wegen $e \geqq 5$ genügt es folglich, die Gültigkeit des Satzes für $p \equiv 21 \pmod{40}$ und $p \equiv 29 \pmod{40}$ zu zeigen. Aus der folgenden Tabelle geht hervor, dass der Satz für alle solchen Primzahlen mit Ausnahme von $p = 61$ und $p = 109$ besteht.

e		p	ψ^*	e		p	ψ^*
5	$50 < p < 72$	61	**7**	51	$5202 < p < 5408$	5261	3
6	$72 < p < 98$	—				5309	3
7	$98 < p < 128$	101	3			5381	3
		109	**11**	55	$6050 < p < 6272$	6101	3
8	$128 < p < 162$	149	3			6221	3
11	$242 < p < 288$	269	7			6229	7
12	$288 < p < 338$	—				6269	3
16	$512 < p < 578$	541	11	56	$6272 < p < 6498$	6301	17
17	$578 < p < 648$	—				6389	3
21	$882 < p < 968$	941	3			6421	11
22	$968 < p < 1058$	1021	7	60	$7200 < p < 7442$	6469	13
26	$1352 < p < 1458$	1381	11			7229	3
		1429	11			7309	19
27	$1458 < p < 1568$	1549	13	70	$9800 < p < 10082$	7349	3
30	$1800 < p < 1922$	1861	7			9829	11
		1901	3			9901	7
31	$1922 < p < 2048$	1949	3			9941	3
		2029	7			9949	19
32	$2048 < p < 2178$	2069	3	75	$11250 < p < 11552$	10061	3
		2141	3			10069	7
36	$2592 < p < 2738$	2621	3	80	$12800 < p < 13122$	11261	3
45	$4050 < p < 4232$	4229	3			11549	3
46	$4232 < p < 4418$	4261	7			12821	3
		4349	3			12829	7
50	$5000 < p < 5202$	5021	3			12941	3
		5101	7			13109	3
		5189	3	99	$19602 < p < 20000$	19661	3
						19709	3
						19861	11
						19949	3

Nagell [3] hat eine Tabelle der kleinsten ungeraden positiven Nichtreste aller Primzahlen $\leqq 257$ publiziert. Aus dieser Tabelle geht hervor, dass der Satz für $e \leqq 4$ gültig ist. Er ist damit vollständig bewiesen.

LITERATUR

1. T. Nagell, *Zahlentheoretische Notizen* I–VI, Videnskapsselskapets Skrifter (fortgesetzt als Skr. Norske Vid. Akad. Oslo), Mat.-naturv. Klasse, 1923, No. 13, 1–25.
2. T. Nagell, *Sur les restes et les 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. L. Rédei, *Die Existenz eines ungeraden quadratischen Nichtrestes mod. p im Intervall* $1, \sqrt{p}$, Acta Sci. Math. Szeged 15 (1953), 12–19.

UNIVERSITÄT UPPSALA, SCHWEDEN