[4] M. Dodson, *Homogeneous additive congruences*, Philos. Trans. Roy. Soc. London, Ser. A, 261 (1967), pp. 163-210.
[5] G. H. Hardy and J. E. Littlewood, *Some problems of 'Partitio Numerorum' (IV): The singular series in Waring's problem and the value of the number $G(k)$*, Math. Zeit. 12 (1922), pp. 161-188.
[6] — — *Some problems of 'Partitio Numerorum' (VIII): The number $\Gamma(k)$ in Waring's problem*, Proc. London Math. Soc. 28 (1928), pp. 518-542.
[7] — and E. M. Wright, *An Introduction to the Theory of Numbers*, Oxford University Press 1960.
[8] K. Norton, *On homogeneous congruences of odd degree*, Ph. D. Thesis, University of Illinois, Urbana, Illinois.
[9] K. Prachar, *Primzahlverteilung*, Berlin 1957.

UNIVERSITY OF AUCKLAND
Auckland, New Zealand
UNIVERSITY OF YORK
York, England

Reçu par la Rédaction le 5. 10. 1968

ACTA ARITHMETICA
XVI (1969)

A note on the least prime quadratic residue (mod p)

by

D. Wolke (Marburg/Lahn)

Let p be an odd prime. By $r_2(p)$ we denote the least prime quadratic residue (mod p) and by $L(s,\chi)$ the L-function formed with the real character $\left(\frac{n}{p}\right)$.

Elliott [2] recently showed: If for an integer $k \geqslant 0$ and a real $c_1 > 0$

$$L(1,\chi) > \frac{c(\log\log p)^k}{\log p}$$

then we have, for every $\varepsilon > 0$,

$$r_2(p) \leqslant c(\varepsilon)p^{\frac{1}{4}(1+\varepsilon)(k+2)^{-1}}.$$

In this note we will sharpen Elliott's result to

THEOREM. *Let $t(p)$ be a positive function with*

$$\text{(H)} \qquad L(1,\chi) > \frac{t(p)}{\log p}.$$

Then, for absolute $c_2, c_3 > 0$

$$\text{(1)} \qquad r_2(p) \leqslant c_2 p^{c_3(t(p))^{-1/2}}$$

holds.

For the proof we need two lemmas.

LEMMA 1. *For every $\varepsilon > 0$, $p \geqslant p_0(\varepsilon)$ and $x = p^{\frac{1}{4}+\varepsilon}$ we have the inequality*

$$\text{(2)} \qquad \sum_{n<x}\left(1-\frac{n}{x}\right)\sum_{d|n}\mu^2(d)\left(\frac{d}{p}\right) > \frac{x}{6}L(1,\chi).$$

For the proof see Elliott [2], (2). The proof rests upon Burgess' estimation for character sums [1], Siegel's theorem (s. [4], IV, § 8) and a method of Linnik–Vinogradov [3].

If one wants to avoid Burgess' deep inequality one can use the Polya–Vinogradov estimation

$$\sum_{n\leqslant x}\left(\frac{n}{p}\right)\ll p^{1/2}\log p$$

instead.

In (2) one has only to replace x by $p^{1/2+\varepsilon}$.

The trival estimation

$$\sum_{n\leqslant x}\left(\frac{n}{p}\right)\ll p$$

leads to (2), where x is replaced by $x=p^{1+\varepsilon}$.

Let $\nu(n)$ denote the number of different prime factors of n, let q denote primes. All the following $\ll$-constants are absolute.

Lemma 2. *For $2\leqslant y\leqslant x$ we have*

$$\sum_{\substack{n\leqslant x\\ q\mid n\to q\geqslant y}} 2^{\nu(n)}\ll\frac{x\log x}{\log^2 y}. \tag{3}$$

Proof. Let the sum on the left side of (3) be called $S(x,y)$. We get

$$S(x,y)=\sum_{\substack{n\leqslant x\\ q\mid n\to q\geqslant y}}\sum_{d\mid n}\mu^2(d)=\sum_{\substack{d\leqslant x\\ q\mid n\to q\geqslant y}}\mu^2(d)\sum_{\substack{n\leqslant x\\ n\equiv 0\,(\mathrm{mod}\,d)\\ q\mid n\to q\geqslant y}}1\leqslant\sum_{\substack{d\leqslant x\\ q\mid n\to q\geqslant y}}\mu^2(d)\sum_{\substack{n\leqslant x/d\\ q\mid n\to q\geqslant y}}1.$$

By Brun's method one can easily prove, for $2\leqslant v\leqslant u$,

$$\Phi(u,v)=\sum_{\substack{n\leqslant u\\ q\mid n\to q\geqslant v}}1\ll u\prod_{p<v}\left(1-\frac{1}{p}\right)\ll\frac{u}{\log v}.$$

Using this in the above inequality we get

$$S(x,y)\ll\sum_{\substack{d\leqslant x\\ q\mid n\to q\geqslant y}}\mu^2(d)\left\{\frac{x}{d\log y}+1\right\}\leqslant\frac{x}{\log y}\prod_{y\leqslant q\leqslant x}\left(1+\frac{1}{q}\right)+\sum_{\substack{n\leqslant x\\ q\mid n\to q\geqslant y}}1$$

$$\ll\frac{x}{\log^2 y}\log x+\frac{x}{\log y}\ll\frac{x\log x}{\log^2 y},\qquad\text{q.e.d.}$$

Proof of the theorem. For $\varepsilon>0$ and $p\geqslant p_0(\varepsilon)$ Lemma 1 gives

$$\frac{x}{6}L(1,\chi)<\sum_{n<x}\left(1-\frac{n}{x}\right)\prod_{q\mid n}\left(1+\left(\frac{q}{p}\right)\right)\leqslant\sum_{\substack{n\leqslant x\\ q\mid n\to(q/p)=1}}2^{\nu(n)}\leqslant\sum_{\substack{n\leqslant x\\ q\mid n\to q\geqslant r_2(p)}}2^{\nu(n)}.$$

We use Lemma 2 and get for absolute $c_4, c_5>0$

$$\frac{x}{6}L(1,\chi)\leqslant c_4\frac{x\log x}{\log^2 r_2(p)}\quad\text{ or }\quad r_2(p)\leqslant\exp\left\{\left(c_5\frac{\log x}{L(1,\chi)}\right)^{1/2}\right\}.$$

We insert the assumption (H), replace x by $p^{1/4+\varepsilon}$ (for a fixed $\varepsilon>0$) and obtain the result.

The notes following Lemma 1 show that for the proof of the theorem the Polya–Vinogradov or even the trivial estimation for character sums is sufficient. In this case the constant c_3 has, if necessary, to be replaced by a larger one.

References

[1] D. A. Burgess, *On character sums and primitive roots*, Proc. London Math. Soc. (3) 12 (1962), pp. 179–192.

[2] P. D. T. A. Elliott, *A note on a recent paper of U. V. Linnik and A. I. Vinogradov*, Acta Arith. 13 (1967), pp. 103–105.

[3] A. I. Vinogradov and Yu. V. Linnik, *Hyperelliptic curves and the least prime quadratic residue*, Dokl. Akad. Nauk SSSR 168 (1966), pp. 259–261.

[4] K. Prachar, *Primzahlverteilung*, Berlin 1957.

Reçu par la Rédaction le 14. 10. 1968

ACTA ARITHMETICA
XVI (1969)

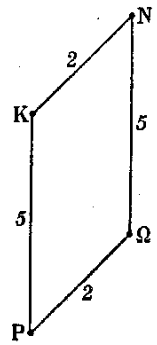
Über den Klassenkörper zum quadratischen Zahlkörper mit der Diskriminante —47

(Fortsetzung)

von

HELMUT HASSE (z. Zt. Honolulu, Hawaii)
und JOSEPH LIANG (Columbus, Ohio)

0. Diese Arbeit knüpft an die Schlußbemerkung einer Arbeit [1] gleichen Titels des erstgenannten Verfassers an. Die dort in Aussicht gestellte Untersuchung wurde inzwischen durch eine gemeinsame Arbeit [2] des zweitgenannten Verfassers mit Zassenhaus in Gang gesetzt, deren



Ergebnisse es uns dann ermöglicht haben, die in jener Schlußbemerkung gestellten Fragen vollständig zu beantworten.

In [1] wurde der Klassenkörper $\mathbf{N}$ zu dem quadratischen Zahlkörper $\mathbf{\Omega} = \mathbf{P}(\sqrt{-47})$ — dem ersten imaginär-quadratischen Zahlkörper mit durch 5 teilbarer Klassenzahl, nämlich $h = 5$ — nach den rein-arithmetischen Methoden der allgemeinen Klassenkörpertheorie numerisch konstruiert.

Man weiß aus der Klassenkörpertheorie, daß $\mathbf{N}/\mathbf{\Omega}$ zyklisch vom Grade 5 und $\mathbf{N}/\mathbf{P}$ normal mit Diedergruppe der Ordnung $2 \cdot 5$ ist. Demnach entsteht $\mathbf{N}$ durch Komposition von $\mathbf{\Omega}$ mit einem nicht-normalen Körper $\mathbf{K}$ vom Grade 5, der als der einzige reelle unter seinen Konjugierten nor-