Proceedings of the Edinburgh Mathematical Society (1996) **39**, 581–588 ©

PROOF OF A CONJECTURE OF HEATH-BROWN CONCERNING QUADRATIC RESIDUES

by R. R. HALL

(Received 3rd March 1995)

The conjecture in question is that the proportion of the first n positive integers which are quadratic residues of an arbitrary prime p is bounded below by a positive. δ. This is established here as a corollary of a more general result concerning multiplicative functions; the problem of the sharp δ is left open.

1991 *Mathematics subject classification.* 11 N 37.

1. Introduction

During the British Mathematical Colloquium in Cardiff, 1994, Roger Heath-Brown informally made the following conjecture. There exists an absolute positive constant δ such that for all primes p and positive integers n, the proportion of the integers not exceeding n which are quadratic residues (mod p) is at least δ.

I shall prove this here, without determining the best possible value of δ, as a corollary of the following more general result.

Theorem. *Let $\mathscr{F}$ denote the class of completely multiplicative arithmetic functions f such that $-1 \leqq f(m) \leqq 1$ for all m. Then*

$$c := \inf\left\{\frac{1}{n}\sum_{m\leqq n} f(m)\colon f\in\mathscr{F}, n\geqq 1\right\} > -1. \tag{1}$$

I have not determined the value of c, but I offer some remarks about this problem in the second section of the paper. To verify Heath-Brown's conjecture we apply the theorem with

$$f(m) = \left(\frac{m}{p}\right),$$

and this yields $\delta \geqq (1+c)/2$. Since we require f to be (completely) multiplicative we must define $f(p)=0$, that is we do not count the multiples of p as quadratic residues.

The proof of the theorem is short, but depends on two hard lemmas. In each of these

https://doi.org/10.1017/S0013091500023324 Published online by Cambridge University Press

I state the best result currently known, (which might be important for the evaluation of c), and then indicate earlier results from the literature which would be sufficient to prove the theorem in its present form.

Lemma 1. *Let g be multiplicative, $-1 \leqq g(m) \leqq 1$ for all m. Then*

$$\sum_{m \leqq x} g(m) \ll x \exp\left\{-K \sum_{p \leqq x} \frac{(1-g(p))}{p}\right\}, \tag{2}$$

where $K = .32867... = -\cos \phi_0$ and ϕ_0 is the (unique) root in $(0, \pi)$ of the equation $\sin \phi - \phi \cos \phi = \pi/2$. The constant K is sharp.

This is due to Hall and Tenenbaum [5]. (See also [4]). Any of the previous results of this sort, with a positive but unsharp K, [3, 1, 8] would do for our present application.

Lemma 2. *Let h be multiplicative, $0 \leqq h(m) \leqq 1$ for all m. Then we have*

$$x^{-1} \sum_{m \leqq x} h(m) \geqq R(h, x)\{\sigma_-(E(h, x))(1 + O \log^{-\alpha} x)) + O(\exp(-\log^{\beta} x))\}$$

where α and β are absolute positive constants, $\sigma_-(E) = E\rho(E)$, ρ being Dickman's function, and

$$R(h, x) = \prod_{p \leqq x} \left(1 - \frac{1}{p}\right)\left(1 + \frac{h(p)}{p} + \frac{h(p^2)}{p^2} + \cdots\right),$$

$$E(h, x) = \exp\left\{\sum_{p \leqq x} \frac{(1-h(p))}{p}\right\}.$$

This is a specialization for our purpose of a difficult result of Hildebrand [6], in which there is a less restricted condition on h; moreover there is an extra variable z at our disposal. We have put $z = 2$. We could obtain Heath-Brown's conjecture, but not our theorem above, with a result of Erdös and Ruzsa [2] on the small sieve, together with one of the weaker versions of Lemma 1.

Proof of the theorem. We begin by considering Lemma 1, and we see that there exists an absolute constant T such that whenever the sum over p on the right of (2) exceeds T, we have

$$-\tfrac{1}{2}x < \sum_{m \leqq x} g(m) < \tfrac{1}{2}x. \tag{3}$$

https://doi.org/10.1017/S0013091500023324 Published online by Cambridge University Press

Let $f \in \mathscr{F}$ and the positive integer n be given. We notice that we may assume that n is large since the quantity inside the curly brackets in (1) is $\geqq -1+2/n$. There are two cases according to whether or not we have

$$\sum_{p \leqq n} \frac{1-f(p)}{p} > T. \tag{4}$$

If (4) holds then we apply Lemma 1 with $g=f$ and $x=n$, when the left-hand inequality in (3) is all we need. Next suppose that (4) does not hold. In this case we define the supplementary, completely multiplicative function h by setting

$$h(p)=\max\{0, f(p)\}, \tag{5}$$

for all primes p. From the negation of (4) and (5) we have

$$\sum_{p \leqq n} \frac{1-h(p)}{p} \leqq T. \tag{6}$$

We apply Lemma 2, writing $S=\exp T$. This yields

$$n^{-1} \sum_{m \leqq n} h(m) \geqq R(h,n)\{\sigma_{-}(S)(1+O(\log^{-\alpha} n))+O(\exp(-\log^{\beta} n)\}. \tag{7}$$

Since h is completely multiplicative and $0 \leqq h(p) \leqq 1$ we have

$$R(h,n)=\prod_{p \leqq n}\left(1-\frac{1-h(p)}{p-h(p)}\right) \geqq \exp\left\{-2\sum_{p \leqq n}\frac{1-h(p)}{p-h(p)}\right\} \geqq \exp\{-2T-B\} \tag{8}$$

in which

$$B=2\sum_{p}\frac{1}{p(p-1)}.$$

It follows that there exist absolute constants $n_0 \in \mathbb{N}$ and $b \in \mathbb{R}^{+}$ such that provided $n > n_0$, the right hand side of (7) is not less than b.

Let $\mathscr{P}=\mathscr{P}(f,n)$ denote the set of primes $p \leqq n$ for which $f(p)$ is negative. We have

$$\sum_{m \leqq n} f(m) \geqq -n+2\sum_{m \leqq n} f(m)\,\chi(m,\mathscr{P}) \tag{9}$$

where $\chi(m,\mathscr{P})$ denotes the characteristic function of the integers free of prime factors in $\mathscr{P}$. We have $f(m)\chi(m,\mathscr{P})=h(m)$ for $m \leqq n$ so that if $n > n_0$ the right hand side of (9) is at least $(2b-1)n$. Put $c_1=\min\{-1+2/n_0, -1/2, 2b-1\}$. We have shown that in every case,

https://doi.org/10.1017/S0013091500023324 Published online by Cambridge University Press

$$n^{-1}\sum_{m\leqq n} f(m)\geqq c_1, \tag{10}$$

which proves our theorem.

2. The value of c

In this section we give an upper bound for c. There are essentially two approaches to this problem. In the first we specify a fairly small numerical value of n together with values of $f(p)$ for $p\leqq n$. For example, we may set $n=3$, $f(2)=f(3)=-1$, to obtain that $c\leqq -1/3$. The method really requires a computer and I have not proceeded very far with it. The second approach, which is more interesting, depends on the asymptotic distribution of the primes. We define

$$c_0=\liminf\left\{\frac{1}{x}\sum_{m\leqq x} f(m)\colon f\in\mathscr{F}\right\},\ (x\to\infty) \tag{11}$$

so that $c\leqq c_0$. In view of the oscillatory behaviour of these sums it is possible that this inequality is strict. We shall prove that $c_0\leqq -.656999\ldots$ in this note.

Let E be a set of primes, possibly depending on x, and put

$$f(p)=-1 \text{ if } p\in E,\ f(p)=+1 \text{ else.} \tag{12}$$

In the usual terminology we therefore have

$$f(m)=(-1)^{\Omega(m,E)}. \tag{13}$$

We shall choose $E=\{p\colon x^{\alpha}<p\leqq x]$, with a particular value of α. The limit

$$\lim\frac{1}{x}\sum_{m\leqq x} f(m),\ (x\to\infty) \tag{14}$$

exists and is an upper bound for c_0. It is convenient to write $\alpha=1/t$ where $t>1$, and to denote the limit in (14) by $R(t)$. We evaluate the quantity $\inf\{R(t)\colon t>1\}$, in fact we show that for all $t>1$ we have

$$R(t)\geqq R(1+\sqrt{e})=-.656999\ldots \tag{15}$$

We require a formula for $R(t)$. It is technically a little easier to deal with the sum

$$S(x,E)=\sum_{m\leqq x}(-1)^{\omega(m,E)} \tag{16}$$

in which $\omega(m,E)$ counts the number of distinct prime factors of m belonging to E; of

https://doi.org/10.1017/S0013091500023324 Published online by Cambridge University Press

course the function in (16) does not belong to $\mathscr{F}$ and so we require the following lemma.

Lemma 3. *Let E be an arbitrary set of primes with least element p_0, and $f(m)$, $S(x,E)$ be as defined in (13) and (16). Then we have*

$$\sum_{m\leqq x} f(m) = S(x,E) + O\left(\frac{1}{p_0 \log p_0}\right). \tag{17}$$

Proof. We may assume that $p_0 \geqq 3$. Let $g(m)$ denote the multiplicative function such that $g(p^r)=0$ if $p\notin E$ and if $p\in E$,

$$g(p^r) = \frac{1}{3}\{2^r + 2(-1)^r\}. \tag{18}$$

Then we have

$$(-1)^{\Omega(m,E)} = \sum_{d\mid m} g(d)(-1)^{\omega(m/d,E)} \tag{19}$$

and so

$$\sum_{m\leqq x} (-1)^{\Omega(m,E)} = \sum_{d\leqq x} g(d) S\left(\frac{x}{d}, E\right). \tag{20}$$

It follows that

$$\begin{aligned}\sum_{m\leqq x} f(m) &= S(x,E) + O\left(x \sum_{d>1} \frac{g(d)}{d}\right)\\ &= S(x,E) + O\left(x\left(\prod_{p\in E}\left(\frac{1-1/p}{1-1/p-2/p^2}\right)-1\right)\right)\end{aligned} \tag{21}$$

which leads to the result stated.

Let $E=\{p: x^\alpha < p \leqq x\}$, with $\alpha>0$ fixed. We have $p_0\to\infty$ and so by Lemma 3, we may evaluate the limit in (14) as if $S(x,E)$ appeared instead of the sum on the left. We write, for $k\geqq 1$,

$$D_k(m;u,v) = \operatorname{card}\{d: d\mid m, d=p_1p_2\dots p_k: u<p_1<p_2<\cdots<p_k\leqq v\}. \tag{22}$$

We define $D_0(m;u,v)=1$ so that we have

$$(-1)^{\omega(m,E)} = \sum_{k=0}^{\infty} (-2)^k D_k(m;u,v) \tag{23}$$

in which $u=x^{1/t}$, $v=x$. For $1\leqq k\leqq t$,

https://doi.org/10.1017/S0013091500023324 Published online by Cambridge University Press

$$\sum_{m\leqq x} D_k(m;u,v)=x\sum_{(k)}\frac{1}{d}+O\left(\frac{x}{\log x}\frac{(\log\log x)^{k-1}}{(k-1)!}\right), \tag{24}$$

where the range of summation in the right-hand sum is as defined in (22), with the additional restriction that $d\leqq x$. We assemble (23) and (24), noticing that since $1/t>0$ by hypothesis, the sums over k are finite. We interpret the sum on the right of (24) as 1 when $k=0$ and we obtain, with suitable K,

$$\sum_{m\leqq x}(-1)^{\omega(m,E)}=x\sum_{k\leqq t}(-2)^k\sum_{(k)}\frac{1}{d}+O\left(\frac{x}{\log x}(\log\log x)^K\right). \tag{25}$$

Our treatment of the inner right-hand sum in (25) is standard and we may omit the details. We find that for each fixed k,

$$\sum_{(k)}\frac{1}{d}=F_k(t)+o(1),\ (x\to\infty) \tag{26}$$

in which $F_0(t)=1$ and for $k\geqq 1$,

$$F_k(t)=\frac{1}{k!}\int_{1/t}^{1}\int_{1/t}^{1}\cdots\int_{1/t}^{1}H(1-x_1-x_2-\cdots-x_k)\frac{dx_1dx_2\ldots dx_k}{x_1x_2\ldots x_k}$$

$$=\frac{1}{k!}\int_{1}^{\infty}\int_{1}^{\infty}\cdots\int_{1}^{\infty}H(t-x_1-x_2-\cdots-x_k)\frac{dx_1dx_2\ldots dx_k}{x_1x_2\ldots x_k}. \tag{27}$$

Here H denotes Heaviside's function, $H(u)=1$ if $u\geqq 0$, $H(u)=0$ else. We assemble (25) and (26) and we see that $S(x,E)=(R(t)+o(1))x$ where

$$R(t)=\sum_{k=0}^{\infty}(-2)^kF_k(t). \tag{28}$$

The sum on the right is finite because $F_k(t)=0$ when $k\geqq t$. We have, from (27), (or by an exercise in Laplace transforms) that

https://doi.org/10.1017/S0013091500023324 Published online by Cambridge University Press

$$t\frac{d}{dt}F_k(t)=\frac{1}{(k-1)!}\int_{1/t}^{1}\int_{1/t}^{1}\cdots\int_{1/t}^{1}H(1-\frac{1}{t}-x_1-\cdots-x_{k-1})\frac{dx_1dx_2\ldots dx_{k-1}}{x_1x_2\ldots x_{k-1}}$$

$$=F_{k-1}(t-1), \tag{29}$$

and we deduce from (28) and (29) that for $t>1$,

$$t\frac{d}{dt}R(t)=-2R(t-1). \tag{30}$$

We set $R(t)=1$ for $0<t\leqq 1$. The differential-difference equation (30) is of a familiar type; perhaps the simplest way to achieve the kind of oscillation result we require is via the adjoint equation and what Iwaniec [7] refers to as the inner product. The adjoint equation is

$$\frac{d}{dt}\{tQ(t)\}=2Q(t+1), \tag{31}$$

and we readily check by differentiation that we have

$$tR(t)Q(t)-2\int_{t-1}^{t}R(u)Q(u+1)du=\text{constant}. \tag{32}$$

Equation (31) has the solution $Q(t)=t-2$, and we insert this into (32) and set $t=1$ to find that the constant on the right is zero. Now define $R^*(t)=\max\{|R(u)|:t-1\leqq u\leqq t\}$. We deduce from (32) that for $t\geqq 2$ we have

$$t(t-2)|R(t)|\leqq 2R^*(t)\int_{t-1}^{t}(u-1)du=(2t-3)R^*(t), \tag{33}$$

whence for $t>3$, $|R(t)|<R^*(t)$. We infer from this that any stationary absolute value of $R(t)$ in the range $t>3$ does not exceed all the previous ones, (we may think of t as time since we are really concerned here with diffusion equations), so that it will suffice to consider the maxima and minima of $R(t)$ in the interval $[1,3]$. From (30), R plainly decreases throughout $[1,2]$; indeed in this interval $R(t)=1-2\log t$. For $2<t\leqq 3$ we therefore have

$$R(t)=1-2\log t+4\int_{2}^{t}\frac{\log(u-1)}{u}du. \tag{34}$$

We see that there is a minimum at $t=1+\sqrt{e}$, moreover this is the maximum absolute

https://doi.org/10.1017/S0013091500023324 Published online by Cambridge University Press

value of R on this interval. It is therefore the global minimum of $R(t)$, and numerical integration gives $R_{\min} = -.656999\ldots$ as stated above.

I would like to thank the referee for his careful reading of this note, which led to some corrections.

REFERENCES

1. P. D. T. A. Elliott, Some remarks about multiplicative functions of modulus <1, in *Analytic Number Theory* (B. C. Berndt, H. G. Diamond, H. Halberstam, A. Hildebrand eds., Progress in Math. **85** Birkhäuser, 1990), 159–164.

2. P. Erdös and I. Z. Ruzsa, On the small sieve 1, *J. Number Theory* **12** (1980), 385–394.

3. G. Halasz, On the distribution of additive and the mean values of multiplicative arithmetic functions, *Studia Sci. Math. Hungar.* **6** (1971), 211–233.

4. R. R. Hall, A sharp inequality of Halasz type for the mean value of a multiplicative arithmetic function, *Mathematika* **42** (1995), 144–157.

5. R. R. Hall and G. Tenenbaum, Effective mean value estimates for complex multiplicative functions, *Math. Proc. Cambridge Philos. Soc.* **110** (1991), 337–351.

6. A. Hildebrand, Quantitative mean value theorems for nonnegative multiplicative functions 2, *Acta Arith.* **48** (1987), 209–260.

7. H. Iwaniec, Rosser's sieve, bilinear forms of the remainder terms, some applications, in *Recent progress in analytic number theory* (H. Halberstam and C. Hooley eds., Academic Press, 1981), 203–230.

8. G. Tenenbaum, *Introduction a la Theorie Analytique et Probabiliste des Nombres* (Institut Elie Cartan **13**, 1990).

Department of Mathematics
University of York
Heslington, York YO1 5DD
England

https://doi.org/10.1017/S0013091500023324 Published online by Cambridge University Press