Journal of Number Theory 131 (2011) 1105–1111

Contents lists available at ScienceDirect

Journal of Number Theory

www.elsevier.com/locate/jnt

On small solutions to quadratic congruences

Igor E. Shparlinski

Department of Computing, Macquarie University, Sydney, NSW 2109, Australia

ARTICLE INFO

Article history:
Received 6 April 2010
Revised 11 November 2010
Accepted 21 December 2010
Available online 16 February 2011
Communicated by Robert C. Vaughan

MSC:
11D79
11J71
11L07

Keywords:
Quadratic congruences
Pair correlation

ABSTRACT

We estimate the deviation of the number of solutions of the congruence

$$m^2 - n^2 \equiv c \pmod q, \quad 1 \leqslant m \leqslant M,\ 1 \leqslant n \leqslant N,$$

from its expected value on average over $c = 1, \dots, q$. This estimate is motivated by the connection, recently established by D.R. Heath-Brown, between the distribution of solution to this congruence and the pair correlation problem for the fractional parts of the quadratic function αk^2, $k = 1, 2, \dots$ with a real α.

1. Introduction

For positive integers M, N and q and an arbitrary integer c, we denote

$$A(M, N; q, c) = \#\{1 \leqslant m \leqslant M,\ 1 \leqslant n \leqslant N:\ m^2 - n^2 \equiv c \pmod q\}.$$

We also put $A_0(q, c) = A(q, q; q, c)$ and define

$$\Delta(M, N; q, c) = \left| A(M, N; q, c) - \frac{MN}{q^2} A_0(q, c) \right|.$$

It has been shown by Heath-Brown [2, Lemma 3] that the bound

E-mail address: igor.shparlinski@mq.edu.au.

0022-314X/$ – see front matter
doi:10.1016/j.jnt.2010.12.002

$$\sum_{c=1}^{q} \Delta(N, N; q, c)^2 \leqslant q^{4/3+o(1)} r^3, \tag{1}$$

holds for $N \leqslant q^{2/3}$, where

$$r = \prod_{p=2 \text{ or } \alpha_p > 1} p^{\alpha_p}$$

and

$$q = \prod_{p|q} p^{\alpha_p}$$

is the prime number factorisation of q. The estimate (1) is a part of the approach of [2] to the pair correlation problem for the fractional parts of the quadratic function αk^2, $k = 1, 2, \ldots$, with a real α.

Here we use a different method that leads to an estimate which improves and generalises (1) for most of the values of the parameters M and N. However, in the case of M, $N = q^{2/3+o(1)}$, which is apparently necessary in the applications to the pair correlation problem both bounds are of essentially the same type (except for the extra factor of r^3 in (1), which, however, is small for a “typical” q).

On the other hand, studying the distribution of solutions to the congruence $m^2 - n^2 \equiv c \pmod q$, in particular, estimating $\Delta(M, N; q, c)$ individually and on average, is of independent interest.

Since there does not seem to be any immediate implications of our estimate for the pair correlation problem, we present it only in the case of odd q. For even q, one can easily obtain a similar result at the cost of some minor technical changes.

Theorem 1. *For any odd $q \geqslant 1$ and positive integers $M, N \leqslant q$, we have*

$$\sum_{c=1}^{q} \Delta(M, N; q, c)^2 \leqslant (M + N)^2 q^{o(1)}.$$

2. Preliminaries

As usual, we use $\varphi(k)$ to denote the Euler function and $\tau(k)$ to denote the divisor function.

Lemma 2. *If q is odd and* $\gcd(c, q) = d$ *then*

$$A_0(q, c) = \sum_{f|d} f \varphi(q/f).$$

Proof. As in [2, Section 3] we note that if an odd q then $A_0(q, c)$ is equal to the number of solutions to the congruence

$$uv \equiv c \pmod q, \quad 1 \leqslant u, v \leqslant q.$$

Now, for every divisor $f|d$ we collect together the solutions (u, v) with $\gcd(u, q) = f$. Writing $u = fw$ with $1 \leqslant w \leqslant q/f$ and $\gcd(w, q/f) = 1$, we see that $uw \equiv c/f \pmod{q/f}$. Thus, for each of the $\varphi(q/f)$ possible values for w, the corresponding value of u is uniquely defined modulo q/f and thus u takes f distinct values in the range $1 \leqslant u \leqslant q$. $\square$

We also need the following well-known consequence of the sieve of Eratosthenes.

Lemma 3. *For any real numbers W and $Z \geqslant 1$ and an integer $s \geqslant 1$, we have*

$$\sum_{\substack{W<k\leqslant W+Z\\ \gcd(k,s)=1}} 1 = \frac{\varphi(s)}{s} Z + O\big(\tau(s)\big).$$

Proof. Using the inclusion–exclusion principle we write

$$\sum_{\substack{W<k\leqslant W+Z\\ \gcd(k,s)=1}} 1 = \sum_{d\mid s} \mu(d) \sum_{\substack{W<k\leqslant W+Z\\ d\mid k}} 1$$

where $\mu(d)$ is the Möbius function, see [1, Section 16.3]. Therefore,

$$\sum_{\substack{W<k\leqslant W+Z\\ \gcd(k,s)=1}} 1 = \sum_{d\mid s} \mu(d)\big(Z/d + O(1)\big) = Z \sum_{d\mid s} \frac{\mu(d)}{d} + O\big(\tau(s)\big).$$

Recalling that

$$\sum_{d\mid s} \frac{\mu(d)}{d} = \frac{\varphi(s)}{s}$$

see [1, Eq. (16.3.1)], we obtain the desired result. $\square$

Using partial summation, we derive from Lemma 3:

Corollary 4. *For any real numbers W and $Z \geqslant 1$ and an integer $s \geqslant 1$, we have*

$$\sum_{\substack{W<k\leqslant W+Z\\ \gcd(k,s)=1}} k = \frac{\varphi(s)}{2s} Z(W+Z) + O\big((W+Z)\tau(s)\big).$$

Finally, we recall the bound

$$\tau(k) = k^{o(1)}, \tag{2}$$

see [1, Theorem 317].

3. Products in residue classes

Here we present our main technical tool. Assume that for an integer s we are given two sequences of nonnegative real numbers

$$\mathcal{Y} = \{Y_u\}_{u=1}^{s} \quad \text{and} \quad \mathcal{Z} = \{Z_u\}_{u=1}^{s}.$$

We denote by $T(X, \mathcal{Y}, \mathcal{Z}; s, a)$ the number of solutions to the congruence

$$uv \equiv a \pmod s, \quad 2 \leqslant u \leqslant X, \qquad \gcd(u,s) = 1, \quad Z_u \leqslant v \leqslant Z_u + Y_u.$$

The following result is an immediate generalisation of [4, Theorem 1], which corresponds to the constant values of the form $Y_u = Y$ and $Z_u = Z + 1$ for some integers Y and Z.

Lemma 5. *Assume that*

$$\max_{2 \leqslant u \leqslant X} Y_u = Y.$$

Then

$$\sum_{a=1}^{s} \left| T(X, \mathcal{Y}, \mathcal{Z}; s, a) - \frac{1}{s} \sum_{\substack{2 \leqslant u \leqslant X \\ \gcd(u,s)=1}} Y_u \right|^2 \leqslant X(X+Y)s^{o(1)}.$$

Proof. We recall that by [3, Bound (8.6)], for $2 \leqslant u \leqslant X$ we have

$$\sum_{Z_u \leqslant v \leqslant Z_u + Y_u} \mathbf{e}_s(ry) \ll \min\{Y_u, s/|r|\} \ll \min\{Y, s/|r|\},$$

which holds for any integer with $0 < |r| \leqslant s/2$. Now the proof of [4, Theorem 1] extends to this more general case without any changes. □

4. Proof of Theorem 1

Without loss of generality we may assume that

$$M \geqslant N. \tag{3}$$

Using the variables $x = m + n$ and $y = m - n$ we see that $A(M, N; q, c)$ is equal to the number of solutions to the congruence

$$xy \equiv c \pmod q, \tag{4}$$

where

$$2 \leqslant x + y \leqslant 2M, \; 2 \leqslant x - y \leqslant 2N, \quad y \equiv x \pmod 2. \tag{5}$$

Putting $\vartheta_x = 0$ if $x \equiv 0 \pmod 2$ and $\vartheta_x = 1$, otherwise, and writing $y = \vartheta_x + 2v$, we see that (4) and (5) are equivalent to

$$x(\vartheta_x + 2v) \equiv c \pmod q, \quad 2 \leqslant x \leqslant X, \; L_x \leqslant v \leqslant U_x, \tag{6}$$

where $X = M + N$ and

$$L_x = \max\left\{1 - \frac{x + \vartheta_x}{2}, \frac{x - \vartheta_x}{2} - N\right\},$$
$$U_x = \min\left\{1 + \frac{x - \vartheta_x}{2}, M - \frac{x + \vartheta_x}{2}\right\}. \tag{7}$$

We note that it is enough to prove that for every $d|q$ we have

$$\sum_{\substack{c=1\\ \gcd(c,q)=d}}^{q} \Delta(M,N;q,c)^2 \leqslant M^2 q^{o(1)}. \tag{8}$$

Now, assume that $\gcd(c,q)=d$.

For every divisor $f|d$, we collect together the solutions to (6) with $\gcd(x,q)=f$ and denote the number of such solutions by $B(M,N;q,c,f)$.

In particular, if $\gcd(c,q)=d$ then we have

$$A(M,N;q,c)=\sum_{f|d} B(M,N;q,c,f).$$

Hence, using Lemma 2, the Cauchy inequality and the bound (2), we derive

$$\Delta(M,N;q,c)^2 \leqslant q^{o(1)} \sum_{f|d} \left| B(M,N;q,c,f) - \frac{MNf\varphi(q/f)}{q^2}\right|^2. \tag{9}$$

To estimate $B(M,N;q,c,f)$, writing $x=fu$ with $\gcd(u,q/f)=1$, and taking into account that since q is odd, we have $\vartheta_x=\vartheta_u$, we see that $B(M,N;q,c,f)$ is equal to the number of solutions to the congruence

$$u(\vartheta_u+2v)\equiv c_f \pmod{q_f}, \tag{10}$$

where

$$2\leqslant u\leqslant X_f, \quad \gcd(u,q_f)=1, \quad L_{fu}\leqslant v\leqslant U_{fu},$$

and

$$c_f=c/f, \qquad q_f=q/f, \qquad X_f=\lfloor X/f\rfloor.$$

We now rewrite (10) as $u(2^{-1}\vartheta_u+v)\equiv 2^{-1}c_f \pmod{q_f}$. Defining $h_{f,u}$ by the conditions

$$2h_{f,u}\equiv\vartheta_u \pmod{q_f}, \quad 0\leqslant h_{f,u}<q_f,$$

we see that

$$B(M,N;q,c,f)=T\big(X_f,\mathcal{Y}_f,\mathcal{Z}_f;q_f,2^{-1}c_f\big), \tag{11}$$

where $T(X,\mathcal{Y},\mathcal{Z};s,a)$ is defined in Section 3 and with the sequences $\mathcal{Y}_f=\{Y_{f,u}\}_{u=1}^{q_f}$ and $\mathcal{Z}_f=\{Z_{f,u}\}_{u=1}^{q_f}$ given by

$$Z_{f,u}=h_{f,u}+L_{fu} \quad\text{and}\quad Y_{f,u}=U_{fu}-L_{fu}.$$

In order to apply Lemma 5 we need to evaluate the main term

$$W_f = \frac{1}{q_f} \sum_{\substack{u=2\\ \gcd(u,q_f)=1}}^{X_f} (U_{fu} - L_{fu}).$$

Recalling the condition (3) and the definition (7), we see that

$$U_{fu} - L_{fu} = \begin{cases} fu + O(1), & \text{if } u \leqslant N_f, \\ N + O(1), & \text{if } N_f < u \leqslant M_f, \\ N + M - fu + O(1), & \text{if } M_f < u \leqslant X_f, \end{cases}$$

where

$$M_f = \lceil M/f \rceil \quad \text{and} \quad N_f = \lceil N/f \rceil.$$

Thus, using Lemma 3 and Corollary 4, we derive

$$\begin{aligned} W_f &= \frac{f}{q_f} \sum_{\substack{u \leqslant N_f\\ \gcd(u,q_f)=1}} u + \frac{N}{q_f} \sum_{\substack{N_f < u \leqslant M_f\\ \gcd(u,q_f)=1}} 1 \\ &\quad + \frac{M+N}{q_f} \sum_{\substack{N_f < u \leqslant M_f\\ \gcd(u,q_f)=1}} 1 - \frac{f}{q_f} \sum_{\substack{M_f < u \leqslant X_f\\ \gcd(u,q_f)=1}} u + O\big(X_f q_f^{-1}\big) \\ &= \frac{f\varphi(q_f)}{2q_f^2} N_f^2 + \frac{N\varphi(q_f)}{q_f^2}(M_f - N_f) \\ &\quad + \frac{(M+N)\varphi(q_f)}{q_f^2}(X_f - M_f) - \frac{f\varphi(q_f)}{2q_f^2}\big(X_f^2 - M_f^2\big) + O\big(X_f q_f^{-1}\tau(q_f)\big). \end{aligned}$$

Thus recalling the values of q_f, M_f, N_f and X_f, the assumption (3) and using (2), we see that

$$\begin{aligned} W_f &= \frac{fN^2\varphi(q_f)}{2q^2} + \frac{fN(M-N)\varphi(q_f)}{q^2} \\ &\quad + \frac{fN(M-N)\varphi(q_f)}{q^2} - \frac{fN(2M-N)\varphi(q_f)}{2q^2} + O\big(Mq^{-1}\tau(q)\big) \\ &= \frac{fMN\varphi(q_f)}{q^2} + O\big(Mq^{-1+o(1)}\big). \end{aligned}$$

Thus, by the Cauchy inequality we have

$$\left| B(M,N;q,c,f) - \frac{MNf\varphi(q/f)}{q^2} \right| \leqslant \big|B(M,N;q,c,f) - W_f\big|^2 + O\big(M^2 q^{-2+o(1)}\big).$$

Therefore, we derive from (9) that

$$\Delta(M,N;q,c)^2 \leqslant q^{o(1)} \sum_{f|d} \left|B(M,N;q,c,f) - W_f\right|^2 + O\left(M^2 q^{-2+o(1)}\right).$$

Hence,

$$\begin{aligned}
\sum_{\substack{c=1\\ \gcd(c,q)=d}}^{q} \Delta(M,N;q,c)^2 &\leqslant \sum_{\substack{c=1\\ \gcd(c,q)=d}}^{q} \sum_{f|d} \left|B(M,N;q,c,f) - W_f\right|^2 + O\left(M^2 q^{-1+o(1)}\right)\\
&\leqslant \sum_{f|d} \sum_{\substack{c=1\\ f|c}}^{q} \left|B(M,N;q,c,f) - W_f\right|^2 + O\left(M^2 q^{-1+o(1)}\right)\\
&\leqslant \sum_{f|d} \sum_{c_f=1}^{q_f} \left|B(M,N;q,fc_f,f) - W_f\right|^2 + O\left(M^2 q^{-1+o(1)}\right).
\end{aligned}$$

Recalling (11) and applying Lemma 5, we obtain (8) and conclude the proof.

Acknowledgments

The author is grateful to Roger Heath-Brown for very useful discussions. During the preparation of this paper, the author was supported in part by ARC grant DP1092835.

References

[1] G.H. Hardy, E.M. Wright, An Introduction to the Theory of Numbers, Oxford Univ. Press, Oxford, 1979.
[2] D.R. Heath-Brown, Pair correlation for fractional parts of αn^2, Math. Proc. Cambridge Philos. Soc. 148 (2010) 385–407.
[3] H. Iwaniec, E. Kowalski, Analytic Number Theory, Amer. Math. Soc., Providence, RI, 2004.
[4] I.E. Shparlinski, Distribution of inverses and multiples of small integers and the Sato–Tate conjecture on average, Michigan Math. J. 56 (2008) 99–111.