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

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

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

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

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*

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

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 $f \mid d$ 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 $1 \leqslant u \leqslant q$. □

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