Available online at www.sciencedirect.com
ScienceDirect
Indagationes Mathematicae 27 (2016) 480–487
indagationes mathematicae
www.elsevier.com/locate/indag

Random congruences

Jörg Brüdern[a,*], Rainer Dietmann[b]

[a] Mathematisches Institut, Bunsenstrasse 3-5, 37073 Göttingen, Germany
[b] Department of Mathematics, Royal Holloway, University of London, Egham, Surrey TW20 0EX, UK

Abstract

The size of the smallest primitive solution of a random congruence is determined.

Keywords: Congruences in general position

1. Introduction

The distribution of small solutions of homogeneous congruences is a theme of some relevance in the theory of numbers, mainly because of an intimate connection with incomplete exponential sums (see for example [1,4,5,7,8]). Here we investigate this theme on average to study the question for a form in general position. In preparation for the announcement of our results, fix a degree $d \in \mathbb{N}$, and write a form $F \in \mathbb{Z}[X_1, \dots, X_s]$ of degree d as

$$F = \sum_{\mathbf{j} \in \mathscr{J}} a_{\mathbf{j}} X_{j_1} \cdots X_{j_d}, \tag{1}$$

where $\mathbf{j} = (j_1, \dots, j_d)$ runs over the set

$$\mathscr{J} = \{\mathbf{j} \in \mathbb{N}^d : j_1 \le \cdots \le j_d \le s\}.$$

* Corresponding author.
E-mail addresses: Joerg.Bruedern@mathematik.uni-goettingen.de (J. Brüdern), Rainer.Dietmann@rhul.ac.uk (R. Dietmann).

http://dx.doi.org/10.1016/j.indag.2015.10.001
0019-3577/

In the sequel we will often signal the dependence of F on $\mathbf{a}$ in (1) by writing $F = F_{\mathbf{a}}$. In this notation, whenever q is a natural number and $1 \le B < q$, let

$$\mathscr{X}(q, B) = \{\mathbf{x} \in \mathbb{Z}^s : |x_j| \le B, (x_j, q) = 1 \quad (1 \le j \le s)\}$$

and

$$N_{\mathbf{a}}(q, B) = \#\{\mathbf{x} \in \mathscr{X}(q, B) : F_{\mathbf{a}}(\mathbf{x}) \equiv 0 \bmod q\}.$$

Note that $\mathbf{0} \notin \mathscr{X}(q, B)$. Thus, any solution of $F_{\mathbf{a}}(\mathbf{x}) \equiv 0 \bmod q$ counted by $N_{\mathbf{a}}(q, B)$ is non-trivial. The problem that we wish to describe is certainly simplest when q is a prime p. A naïve statistical heuristics would suggest that $N_{\mathbf{a}}(p, B)$ should roughly be of size $(2B)^s/p$ provided only that this last quantity is large. This prediction is certainly false for some forms, as we shall show momentarily by means of a simple example. However, in a suitable mean square sense, one can show that the proportion of forms where $N_{\mathbf{a}}(p, B) - (2B)^s/p$ is small tends to 1 as p grows. Such a result can be substantiated for a larger class of moduli, and therefore, we now return to the discussion of general $q \in \mathbb{N}$, and move on to describe the averaging process over sets of forms. Informally speaking, we allow the coefficients $a_{\mathbf{j}}$ to range over a complete set of residues, modulo q, or put them to 0. The "diagonal" coefficients $a_{(j,j,\dots,j)}$ will always range over $\{1, 2, \dots, q\}$. More precisely, associate with each $\mathbf{j} \in \mathscr{J}$ a set $\mathscr{A}_{\mathbf{j}} \subset \{1, \dots, q\}$. We refer to a family $\mathfrak{A} = (\mathscr{A}_{\mathbf{j}})_{\mathbf{j} \in \mathscr{J}}$ of such sets as *admissible* if for each $\mathbf{j} \in \mathscr{J}$ the set $\mathscr{A}_{\mathbf{j}}$ is one of the two sets $\{1, \dots, q\}$ or $\{q\}$, and for all $\mathbf{j} = (j, j, \dots, j)$ with $1 \le j \le s$ one has $\mathscr{A}_{\mathbf{j}} = \{1, \dots, q\}$. By slight abuse of notation, we shall write $\mathbf{a} \in \mathfrak{A}$ as a shorthand for the assertion that $a_{\mathbf{j}} \in \mathscr{A}_j$ holds for all $\mathbf{j} \in \mathscr{J}$. With this convention understood, we also write

$$\#\mathfrak{A} = \sum_{\mathbf{a} \in \mathfrak{A}} 1.$$

Note that whenever $\mathfrak{A}$ is admissible, and one has $\mathscr{A}_{\mathbf{j}} = \{1, \dots, q\}$ for exactly J of the indices $\mathbf{j} \in \mathscr{J}$, then $\#\mathfrak{A} = q^J$.

Our primary concern is an estimate for the variance

$$V = \sum_{\mathbf{a} \in \mathfrak{A}} \left(N_{\mathbf{a}}(q, B) - \frac{\#\mathscr{X}(q, B)}{q} \right)^2. \tag{2}$$

This expression measures the difference of $N_{\mathbf{a}}(q, B)$ to its expected size in mean over the family $\mathfrak{A}$. Note that the case where all $\mathscr{A}_{\mathbf{j}}$ are a complete set of residues modulo q is admissible, so that we may average over *all* forms of fixed degree. Also, we may take $\mathscr{A}_{\mathbf{j}} = \{q\}$ for all $\mathbf{j}$ except when all coordinates of $\mathbf{j}$ are equal. This example corresponds to the set of all diagonal forms.

In the statement of our results, it is convenient, for given $0 < \delta \le 1$, to define a positive integer q as δ*-rough* if q has no prime factor smaller than q^δ.

Theorem. *Let $s \ge 3$ and $0 < \delta \le 1$. There exists a number $C = C(d, s, \delta)$ with the property that whenever $\mathfrak{A}$ is admissible and q is δ-rough with $q^{1/s} \le B < q$, then*

$$V \le \frac{C\#\mathfrak{A}}{q^2} \left(B^s q + B^{2s} q^{\delta(2-s)} \right). \tag{3}$$