

*This is a review submitted to Mathematical Reviews/MathSciNet.*

**Reviewer Name:** Konstantopoulos, Takis

**Mathematical Reviews/MathSciNet Reviewer Number:** 68397

**Address:**

Department of Mathematics  
Uppsala University  
PO Box 480  
SE-75106 Uppsala  
SWEDEN  
takiskonst@gmail.com

**Author:** Brudern, Jorg; Dietmann, Rainer

**Title:** Random congruences.

**MR Number:** MR3479167

**Primary classification:**

**Secondary classification(s):**

**Review text:**

amsmath,amsthm,amsfonts,amssymb,mathrsfs,epsfig,bm

Given a set of coefficients  $\mathbf{a} = \{a_{j_1, \dots, j_d}\}$ , let  $F_{\mathbf{a}}(X_1, \dots, X_s)$  be a homogeneous polynomial in  $s$  variables of degree  $d$ , that is,

$$F_{\mathbf{a}}(X_1, \dots, X_s) = \sum_{1 \leq j_1 \leq \dots \leq j_d \leq s} a_{j_1, \dots, j_d} X_{j_1} \cdots X_{j_d}.$$

Let  $q > 1$  be a positive integer,  $1 \leq B < q$ , and let  $X(q, B)$  be the set of all integer  $s$ -tuples  $(x_1, \dots, x_s)$  such that  $-B \leq x_j \leq B$  and  $\gcd(x_j, q) = 1$  for all  $j$ . Let  $N_{\mathbf{a}}(q, B)$  be the number of  $(x_1, \dots, x_s) \in X(q, B)$  that satisfy

$$F_{\mathbf{a}}(x_1, \dots, x_s) \equiv 0 \pmod{q}.$$

A set  $\mathbf{a}$  of coefficients is called admissible if the coefficients range over a complete set of residues (mod  $q$ ) or some of the diagonal coefficients  $a_{j, \dots, j}$  are set equal to 0. Let  $\mathfrak{A}$  be the set of admissible coefficients. Then

$$\sum_{\mathbf{a} \in \mathfrak{A}} N_{\mathbf{a}}(q, B) = \frac{|\mathfrak{A}| |X(q, B)|}{q}.$$

It makes sense then to consider

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

as a “variance” (that is,  $V/|\mathfrak{A}|$  is the variance of the random variable  $N_{\mathbf{a}}(q, B)$  when  $\mathbf{a}$  is chosen uniformly at random from  $\mathfrak{A}$ ). The main result is the following

bound for  $V$ . If  $s \geq 3$  and  $0 < \delta \leq 1$ , there exists constant  $C$  such that if  $q$  contains no prime factors less than  $q^\delta$  and  $q^{1/s} \leq B < q$  then

$$V \leq \frac{C|\mathfrak{A}|}{q^2}(B^s q + B^{2s} q^{\delta(2-s)}).$$

An application to the geometry of numbers is also given.

**Comments to the MR Editors (not part of the Review Text):**

The paper requires the use of a curly X. I used the command `X` It didn't work on your system. I indicated the packages I use, the one responsible for this is `mathrsfs`. Still, it didn't work.