Distribution of Matrices with Restricted Entries over Finite Fields

Omran Ahmadi
Department of Electrical and Computer Engineering
University of Toronto, Toronto, ON M5S 3G4, Canada
oahmadid@comm.utoronto.ca

Igor E. Shparlinski
Department of Computing
Macquarie University, Sydney, NSW 2109, Australia
igor@ics.mq.edu.au

January 10, 2007

Abstract

For a prime p, we consider some natural classes of matrices over a finite field $\mathbb{F}_p$ of p elements, such as matrices of given rank or with characteristic polynomial having irreducible divisors of prescribed degrees. We demonstrate two different techniques which allow us to show that the number of such matrices in each of these classes and also with components in a given subinterval $[-H, H] \subseteq [-(p-1)/2, (p-1)/2]$ is asymptotically close to the expected value.

1 Introduction

For integer numbers m and n we use $\mathcal{M}_{m,n}(\mathbb{F}_p)$ to denote the set of $m \times n$ matrices over the field $\mathbb{F}_p$ of p elements where p is a prime.

We always assume that $\mathbb{F}_p$ is represented by the elements of the set $\{0, \pm 1, \ldots, \pm(p-1)/2\}$. Accordingly given a positive integer $H \le (p-1)/2$

we use $\mathcal{M}_{m,n}(H;\mathbb{F}_p)$ to denote the set of $(2H+1)^{n^2}$ matrices $X = (x_{ij})_{m\times n} \in \mathcal{M}_{m,n}(\mathbb{F}_p)$, with $|x_{ij}| \le H$ for $1 \le i \le m$ and $1 \le j \le n$.

For square matrices we also put

$$\mathcal{M}_n(\mathbb{F}_p) = \mathcal{M}_{n,n}(\mathbb{F}_p) \qquad \text{and} \qquad \mathcal{M}_n(H;\mathbb{F}_p) = \mathcal{M}_{n,n}(H;\mathbb{F}_p).$$

Let $\mathcal{T}_n$ be the set of vectors $\mathbf{t} = (t_1, \ldots, t_n)$ with nonnegative integer components such that

$$\sum_{j=1}^{n} t_j j = n.$$

We say that a polynomial f of degree n over $\mathbb{F}_p$ is of *factorisation pattern* $\mathbf{t} \in \mathcal{T}_n$ if it has exactly t_j irreducible factors of degree j, $j = 1, \ldots, n$. For example, $\mathbf{t} = (0, \ldots, 0, 1)$ corresponds to irreducible polynomials and $\mathbf{t} = (n, 0, \ldots, 0)$ corresponds to polynomials which split in $\mathbb{F}_p$.

Motivated by a work of I. Rivin [17], we study various questions about the distribution of matrices $X \in \mathcal{M}_{m,n}(H;\mathbb{F}_p)$. Another motivation for our work comes from the results of W. Duke, Z. Rudnick and P. Sarnak [6] which yield an asymptotic formula for the number of matrices in $\mathrm{SL}_n(\mathbb{Z})$ of restricted Euclidean norm, as well as from a recent extension of these results (in the case $n = 2$) to algebraic number fields by C. Roettger [18]. More precisely, we obtain asymptotic formulas

- for the number $R_{m,n}(k, H;\mathbb{F}_p)$ of matrices $X \in \mathcal{M}_{m,n}(H;\mathbb{F}_p)$ of rank at most $\mathrm{rk}\, X \le k$,
- for the number $F_{n,\mathbf{t}}(H;\mathbb{F}_p)$ of matrices $X \in \mathcal{M}_n(H;\mathbb{F}_p)$ whose characteristic polynomial f has a prescribed factorisation pattern $\mathbf{t} \in \mathcal{T}_n$, and
- for the number $U_n(H;\mathbb{F}_p)$ of matrices $X \in \mathcal{M}_n(H;\mathbb{F}_p)$ with $\det X = 1$, that is, the number of matrices $X \in \mathcal{M}_n(H;\mathbb{F}_p) \cap \mathrm{SL}_n(\mathbb{F}_p)$.

As we have mentioned these questions are $\mathbb{F}_p$ analogues of the results of similar spirit for matrices over $\mathbb{Z}$ and algebraic number fields, see [6, 17, 18] and references therein.

We use these problems to demonstrate several techniques which can be applied to many other similar questions and allow us to show that the number of matrices in certain classes and also with components in a given subinterval

$[-H, H] \subseteq [-(p-1)/2, (p-1)/2]$ is asymptotically close to the expected value.

Throughout the paper, the implied constants in the symbols 'O', and '$\ll$' may depend on integer parameters k and d. We recall that the notations $U = O(V)$ and $U \ll V$ are all equivalent to the assertion that the inequality $|U| \le cV$ holds for some constant $c > 0$.

2 Preparations

2.1 Determinant Varieties

Let $X = (x_{ij})_{m\times n}$ be the $m \times n$ matrix in variables $x_{11}, \ldots, x_{mn}$, and let $I \trianglelefteq \mathbb{C}[x_{11}, \ldots, x_{mn}]$ be the ideal generated by $(k+1) \times (k+1)$ minors of X. Now let the affine set $\mathcal{V}_k(I)$ be the set containing zeros of I in $\mathbb{C}^{mn}$. It is easy to see that the algebraic set $\mathcal{V}_k(I)$ can be identified with $\mathcal{M}_{m\times n}(\mathbb{C}; k)$ where $\mathcal{M}_{m\times n}(\mathbb{C}; k)$ denotes the set of $m \times n$ matrices over $\mathbb{C}$ of rank at most k.

We say that an algebraic variety is not contained in a hyperplane if it is not contained in the zero set of an ideal in $\mathbb{C}[x_{11}, \ldots, x_{mn}]$ generated by a nontrivial linear form in $x_{11}, \ldots, x_{mn}$.

We need the following well-known result (for a simple proof see [1]) which is crucial in what follows.

Lemma 1. *The set $\mathcal{V}_k(I)$ is an irreducible variety of dimension $k(m+n-k)$ in $\mathbb{C}^{mn}$ and it is not contained in a hyperplane.*

Let $\mathcal{U}_n$ be the affine set in $\mathbb{C}[x_{11}, \ldots, x_{nn}]$ associated with $\mathrm{SL}_n(\mathbb{C})$ matrices, that is the zero set of the equation $\det X = 1$ where $X = (x_{ij})_{n\times n}$. We have the following analogue of Lemma 1, see [2, Chapter I, Section 1.6] or [16, Chapter 3, Example 2.12], which in fact can easily be derived from Lemma 1 by examining degrees of possible factors of the polynomial $\det X - 1$.

Lemma 2. *The set $\mathcal{U}_n$ is an irreducible variety of dimension $n^2 - 1$ in $\mathbb{C}^{n^2}$ and it is not contained in a hyperplane.*

2.2 Distribution of Points on Varieties

Now let $\mathcal{F} = \{F_1, F_2, \ldots, F_r\}$ be a family of r polynomials over $\mathbb{Z}$ in s variables. The set of solutions over $\mathbb{C}$ or $\mathbb{F}_p$ to the system of equations

$$F_j(a_1, \ldots, a_s) = 0, \qquad j = 1, \ldots, r,$$

is called the zero set of $\mathcal{F}$ over $\mathbb{C}$ or $\mathbb{F}_p$, respectively.

Let $\mathcal{Z}_{\mathcal{F}}(H;\mathbb{F}_p)$ be the set of vectors $(a_1, a_2, \ldots, a_s) \in \mathbb{F}_p^s$ with $|a_i| \le H$, $i = 1, 2, \ldots, s$ which are in the zero set of $\mathcal{F}$ over $\mathbb{F}_p$. We also put

$$\mathcal{Z}_{\mathcal{F}}(\mathbb{F}_p) = \mathcal{Z}_{\mathcal{F}}((p-1)/2;\mathbb{F}_p).$$

We need the following slight modification of a result of Fouvry [7].

Lemma 3. *Suppose that the affine zero-set of $\mathcal{F} = \{F_1, F_2, \ldots, F_r\}$ in $\mathbb{C}^s$ is an irreducible variety of dimension d and is not contained in a hyperplane of $\mathbb{C}^s$. Then*

$$\begin{aligned}\#\mathcal{Z}_{\mathcal{F}}(H;\mathbb{F}_p) &= \#\mathcal{Z}_{\mathcal{F}}(\mathbb{F}_p)\left(\frac{2H+1}{p}\right)^s \\ &\quad + O\left(p^{d/2}(\log p)^s + H^{d-1}p^{1/2}(\log p)^{s-d+1}\right).\end{aligned}$$

For an s-dimensional vector $\mathbf{a} = (a_1, \ldots, a_s) \in \mathbb{F}_p^s$, we use $T_s(\mathbf{a}, H; p)$ to denote the number of $\lambda \in \mathbb{F}_p^*$ for which

$$a_j\lambda \equiv b_j \pmod p, \text{ with } |b_j| \le H, \qquad j = 1, \ldots, s.$$

The following result is a special case of several more general results which are essentially due to N. M. Korobov [9], which can also be found in many other works, see, for example, [14, 15]. We present it in a form which immediately follows from [15, Theorems 5.6 and 5.10].

Lemma 4. *We have*

$$\sum_{\mathbf{a}\in\mathbb{F}_p^s}\left|T_s(\mathbf{a}, H; p) - \frac{(2H+1)^s}{p^s}(p-1)\right| \ll p^s(\log p)^s.$$

Let $r_{m,n}(k;\mathbb{F}_p)$ be the total number of $m \times n$ matrices of rank k over $\mathbb{F}_p$.

The following explicit formula for $r_{m,n}(k;\mathbb{F}_p)$ is well known, see, for example, [13] for this and many other related formulas.

Lemma 5. *For any $k \ge 0$, we have,*

$$r_{m,n}(k;\mathbb{F}_p) = \frac{\prod_{i=0}^{k-1}(p^m - p^i)\prod_{i=0}^{k-1}(p^n - p^i)}{\prod_{i=0}^{k-1}(p^k - p^i)}.$$

For a monic polynomial $f \in \mathbb{F}_p[T]$ of degree n, we denote by $\mathcal{G}_n(f;\mathbb{F}_p)$ the set of matrices $X \in \mathcal{M}_n(\mathbb{F}_p)$ whose characteristic polynomial is equal to f.

By a result of Chavdarov [3, Theorem 3.9], if $f(0) \neq 0$, then

$$(p-3)^{n^2-n} \leq \#\mathcal{G}_n(f;\mathbb{F}_p) \leq (p+3)^{n^2-n}.$$

Therefore we obtain the following estimate.

Lemma 6. *Let $f \in \mathbb{F}_p[T]$ be a monic polynomial of degree n, and let $f(0) \neq 0$. Then*

$$\#\mathcal{G}_n(f;\mathbb{F}_p) = p^{n^2-n} + O(p^{n^2-n-1}).$$

Notice that polynomials in the above lemma correspond to matrices in $\mathrm{GL}_n(\mathbb{F}_p)$, the general linear group over $\mathbb{F}_p$.

Finally, for $\mathbf{t} \in \mathcal{T}_n$ we denote by $\mathcal{F}_n(\mathbf{t};\mathbb{F}_p)$ the set of monic polynomials $f \in \mathbb{F}_p[T]$ with a factorisation pattern $\mathbf{t}$.

It is well-known (see, for example, [4, 5, 19, 20]) that simple counting arguments imply the following asymptotic formula for the cardinality of $\mathcal{F}_n(\mathbf{t};\mathbb{F}_p)$.

Lemma 7. *For every $\mathbf{t} = (t_1, \ldots, t_n) \in \mathcal{T}_n$, we have*

$$\#\mathcal{F}_n(\mathbf{t};\mathbb{F}_p) = p^n \prod_{j=1}^{n} \frac{1}{t_j! j^{t_j}} + O(p^{n-1}).$$

2.3 Distribution of Products

Let $N_a(H,p)$ denote the number of solutions to the congruence

$$xy \equiv a \pmod{p}, \qquad |x|, |y| \leq H.$$

The following bound on the average deviation between $N_a(H,p)$ and its expected value taken over $|a| \leq (p-1)/2$ is a special case of a more general estimate from [21] (and also the trivial estimate $N_a(H,p) = O(H)$).

Lemma 8. *We have,*

$$\sum_{a=-(p-1)/2}^{(p-1)/2} \left| N_a(H,p) - \frac{(2H+1)^2}{p} \right|^2 \ll H^2 p^{o(1)}.$$

3 Results

3.1 Ranks of Matrices of Bounded Height

Theorem 9. *For $1 \le H \le (p-1)/2$ and $k \le \min\{m,n\}$, we have*

$$R_{m,n}(k,H;\mathbb{F}_p) = (2H+1)^{mn}\, p^{-(m-k)(n-k)} + O\left(p^{k(m+n-k)/2}(\log p)^{mn} + H^{k(m+n-k)-1}p^{1/2}(\log p)^{(m-k)(n-k)+1}\right).$$

Proof. From Lemma 1 and Lemma 3, applied with

$$r = \binom{m}{k}\binom{n}{k}, \qquad s = mn, \qquad d = k(m+n-k),$$

we infer that

$$R_{m,n}(k,H;\mathbb{F}_p) = R_{m,n}(k;\mathbb{F}_p)\left(\frac{2H+1}{p}\right)^{mn} + O\left(p^{k(m+n-k)/2}(\log p)^{mn} + H^{k(m+n-k)-1}p^{1/2}(\log p)^{(m-k)(n-k)+1}\right).$$

By Lemma 5 we see that

$$R_{m,n}(k;\mathbb{F}_p) = \sum_{\ell=0}^{k} r_{m,n}(\ell;\mathbb{F}_p) = p^{k(m+n-k)} + O\left(p^{k(m+n-k)-1}\right)$$

which implies the desired result. □

One can easily see that Theorem 9 is nontrivial whenever

$$H \ge p^{\gamma_{k,m,n}+\varepsilon}$$

where

$$\gamma_{k,m,n} = \max\left\{1/2 + \frac{(m-k)(n-k)}{mn}, 1 - \frac{1}{2(m-k)(n-k)+2}\right\}$$

for some fixed $\varepsilon > 0$ and sufficiently large p. Specially when $m = n$ and $k = n-1$ (the case of singular matrices), then the result is nontrivial whenever

$$H \ge p^{3/4+\varepsilon}.$$

3.2 Factors of Characteristic Polynomials of Matrices of Bounded Height

Theorem 10. *For $1 \le H \le (p-1)/2$ and $\mathbf{t} \in \mathcal{T}_n$, we have*

$$F_{n,\mathbf{t}}(H;\mathbb{F}_p) = (2H+1)^{n^2} \prod_{j=1}^{n} \frac{1}{t_j! j^{t_j}} + O\left(p^{n^2-1}(\log p)^{n^2}\right).$$

Proof. Clearly, if $f(T) \in \mathbb{F}_p[T]$ is the characteristic polynomial of $X \in \mathcal{M}_n(\mathbb{F}_p)$, then for every $\lambda \in \mathbb{F}_p^*$, the characteristic polynomial of $\lambda X \in \mathcal{M}_n(\mathbb{F}_p)$ is $\lambda^n f(T\lambda^{-1})$ and thus has the same factorisation pattern. Therefore

$$\begin{aligned} F_{n,\mathbf{t}}(H;\mathbb{F}_p) &= \frac{1}{p-1} \sum_{f \in \mathcal{F}_n(\mathbf{t};\mathbb{F}_p)} \sum_{X \in \mathcal{G}_n(f;\mathbb{F}_p)} \sum_{\substack{\lambda \in \mathbb{F}_p^* \\ \lambda X \in \mathcal{M}_n(H;\mathbb{F}_p)}} 1 \\ &= \frac{(2H+1)^{n^2}}{p^{n^2}} \sum_{f \in \mathcal{F}_n(\mathbf{t};\mathbb{F}_p)} \sum_{X \in \mathcal{G}_n(f;\mathbb{F}_p)} 1 \\ &\quad + \sum_{f \in \mathcal{F}_n(\mathbf{t};\mathbb{F}_p)} \sum_{X \in \mathcal{G}_n(f;\mathbb{F}_p)} \left(\frac{1}{p-1} \sum_{\substack{\lambda \in \mathbb{F}_p^* \\ \lambda X \in \mathcal{M}_n(H;\mathbb{F}_p)}} 1 - \frac{(2H+1)^{n^2}}{p^{n^2}} \right). \end{aligned}$$

Using Lemmas 6 and 7, we derive

$$\begin{aligned} \sum_{f \in \mathcal{F}_n(\mathbf{t};\mathbb{F}_p)} \sum_{X \in \mathcal{G}_n(f;\mathbb{F}_p)} 1 &= \sum_{\substack{f \in \mathcal{F}_n(\mathbf{t};\mathbb{F}_p) \\ f(0) \neq 0}} \sum_{X \in \mathcal{G}_n(f;\mathbb{F}_p)} 1 + O\left(\sum_{\substack{X \in \mathcal{M}_n(\mathbb{F}_p) \\ X \text{ singular}}} 1 \right) \\ &= \sum_{\substack{f \in \mathcal{F}_n(\mathbf{t};\mathbb{F}_p) \\ f(0) \neq 0}} \left(p^{n^2-n} + O(p^{n^2-n-1}) \right) + O\left(p^{n^2-1}\right) \\ &= p^{n^2-n} \sum_{\substack{f \in \mathcal{F}_n(\mathbf{t};\mathbb{F}_p) \\ f(0) \neq 0}} 1 + O\left(p^{n^2-1}\right) \\ &= p^{n^2} \prod_{j=1}^{n} \frac{1}{t_j! j^{t_j}} + O(p^{n^2-1}), \end{aligned}$$

since obviously

$$\sum_{\substack{f\in\mathcal{F}_n(\mathbf{t};\mathbb{F}_p)\\ f(0)\neq 0}} 1 = \sum_{f\in\mathcal{F}_n(\mathbf{t};\mathbb{F}_p)} 1 + O(p^{n-1}).$$

On the other hand, using Lemma 4, we estimate

$$\begin{aligned}
&\left|\sum_{f\in\mathcal{F}_n(\mathbf{t};\mathbb{F}_p)}\sum_{X\in\mathcal{G}_n(f;\mathbb{F}_p)}\left(\frac{1}{p-1}\sum_{\substack{\lambda\in\mathbb{F}_p^*\\ \lambda X\in\mathcal{M}_n(H;\mathbb{F}_p)}} 1-\frac{(2H+1)^{n^2}}{p^{n^2}}\right)\right| \\
&\qquad\le \sum_{f\in\mathcal{F}_n(\mathbf{t};\mathbb{F}_p)}\sum_{X\in\mathcal{G}_n(f;\mathbb{F}_p)}\left|\frac{1}{p-1}\sum_{\substack{\lambda\in\mathbb{F}_p^*\\ \lambda X\in\mathcal{M}_n(H;\mathbb{F}_p)}} 1-\frac{(2H+1)^{n^2}}{p^{n^2}}\right| \\
&\qquad\le \frac{1}{p-1}\sum_{X\in\mathcal{M}_n(\mathbb{F}_p)}\left|\sum_{\substack{\lambda\in\mathbb{F}_p^*\\ \lambda X\in\mathcal{M}_n(H;\mathbb{F}_p)}} 1-\frac{(2H+1)^{n^2}}{p^{n^2}}(p-1)\right| \\
&\qquad\ll p^{n^2-1}(\log p)^{n^2},
\end{aligned}$$

which concludes the proof. □

One can easily see that Theorem 10 is nontrivial whenever

$$H \ge p^{1-1/n^2+\varepsilon}$$

for some fixed $\varepsilon > 0$ and sufficiently large p.

3.3 Matrices of Bounded Height in $\mathrm{SL}_n(\mathbb{F}_p)$

Following the same arguments as in the proof of Theorem 9 and using Lemma 2 instead of Lemma 1 and recalling that

$$\#\mathrm{SL}_n(\mathbb{F}_p) = \frac{1}{p-1}\#\mathrm{GL}_n(\mathbb{F}_P) = \frac{1}{p-1}\prod_{i=0}^{n-1}(p^n-p^i) = p^{n^2-1}+O(p^{n^2-2}),$$

we immediately obtain:

Theorem 11. *For $1 \le H \le (p-1)/2$, we have*

$$U_n(H;\mathbb{F}_p) = \frac{(2H+1)^{n^2}}{p} + O\left(H^{n^2-2}p^{1/2}(\log p)^2\right).$$

The bound of Theorem 11 is nontrivial if

$$H \ge p^{3/4+\varepsilon}.$$

for any fixed $\varepsilon > 0$ and sufficiently large p.

However for $n = 2$ a different argument leads to a stronger result.

Theorem 12. *For $1 \le H \le (p-1)/2$, we have*

$$U_2(H;\mathbb{F}_p) = \frac{(2H+1)^4}{p} + O\left(H^2 p^{o(1)}\right).$$

Proof. Let us define

$$\Delta_a(H,p) = N_a(H,p) - \frac{(2H+1)^2}{p}$$

and note that

$$\sum_{a=-(p-1)/2}^{(p-1)/2} \Delta_a(H,p) = \sum_{a=-(p-1)/2}^{(p-1)/2} \Delta_{a+1}(H,p) = 0.$$

Then we have

$$\begin{aligned} U_2(H;\mathbb{F}_p) &= \sum_{a=-(p-1)/2}^{(p-1)/2} N_a(H,p)N_{a+1}(H,p) \\ &= \sum_{a=-(p-1)/2}^{(p-1)/2} \left(\frac{(2H+1)^2}{p} + \Delta_a(H,p)\right)\left(\frac{(2H+1)^2}{p} + \Delta_{a+1}(H,p)\right) \\ &= \frac{(2H+1)^4}{p} + \sum_{a=-(p-1)/2}^{(p-1)/2} \Delta_a(H,p)\Delta_{a+1}(H,p). \end{aligned}$$

Bu the Cauchy inequalty

$$\sum_{a=-(p-1)/2}^{(p-1)/2} \Delta_a(H,p)\Delta_{a+1}(H,p)$$
$$\leq \sqrt{\sum_{a=-(p-1)/2}^{(p-1)/2} \Delta_a(H,p)^2}\sqrt{\sum_{a=-(p-1)/2}^{(p-1)/2} \Delta_a(H,p)^2}$$
$$= \sum_{a=-(p-1)/2}^{(p-1)/2} \Delta_a(H,p)^2.$$

Now an application of Lemma 8 concludes the proof. □

Clearly Theorem 12 is nontrivial if

$$H \geq p^{1/2+\varepsilon}.$$

for any fixed $\varepsilon > 0$ and sufficiently large p.

4 Comments

Analogues of Theorem 9 can be proven about the symmetric matrices over $\mathbb{F}_p$. More precisely, suppose that $Y = (y_{ij})_{n\times n}$ is the $n \times n$ symmetric matrix in variables $y_{ij} = y_{ji}$ for $1 \leq i \leq j \leq n$, and let $I \trianglelefteq \mathbb{C}[y_{11}, \ldots, y_{nn}]$ be the ideal generated by $(k+1) \times (k+1)$ minors of Y. Also suppose that $\mathcal{W}_k(I)$ is the set containing zeros of I in $\mathbb{C}^{\binom{n+1}{2}}$. Notice that $\mathcal{W}_k(I)$ can be identified with the set of symmetric $n \times n$ matrices over $\mathbb{C}$ of rank at most k. It follows that (see [10]) $\mathcal{W}_k(I)$ is an irreducible variety in $\mathbb{C}^{\binom{n+1}{2}}$ and is not contained in a hyperplane. Thus applying Lemma 3 one can get similar results as Theorem 9 for symmetric matrices over $\mathbb{F}_p$.

The determinant variety is not smooth, so the results about the distribution of points on such varieties, see [8, 11, 12, 22, 23] and references therein, do not apply.

Acknowledgements

The authors wish to thank Igor Rivin for many stimulating discussions.

This paper was initiated during a very enjoyable visit of the both authors at the Fields Institute; its support and stimulating research atmosphere are gratefully appreciated. Research of I. S. was supported by ARC grant DP0556431.

References

[1] S. S. Abhyankar, 'Combinatoire des tableaux de Young, variétés déterminantielles et calcul de fonctions de Hilbert', *Rend. Sem. Mat. Univ. Politec. Torino*, **42** (1984), 65–88.

[2] A. Borel, *Linear algebraic groups*, Graduate Texts in Mathematics, vol. 126, Springer-Verlag, Berlin, 2nd ed., 1991.

[3] N. Chavdarov, 'The generic irreducibility of the numerator of the zeta function in a family of curves with large monodromy', *Duke Math. J.*, **78** (1997), 151–180.

[4] S. D. Cohen, 'The distribution of polynomials over finite fields', *Acta Arithm.*, **20** (1972), 53–62.

[5] S. D. Cohen, 'Uniform distribution of polynomials over finite fields', *J. London Math. Soc.*, **6**(1972), 93–102.

[6] W. Duke, Z. Rudnick and P. Sarnak, 'Density of integer points on affine homogeneous varieties', *Duke Math. J.*, **71** (1993), 143–179.

[7] É. Fouvry, 'Consequences of a result of N. Katz and G. Laumon concerning trigonometric sums', *Israel J. Math.*, **120** (2000), 81–96.

[8] É. Fouvry and N. Katz, 'A general stratification theorem for exponential sums, and applications', *J. Reine Angew. Math.*, **540** (2001), 115–166.

[9] N. M. Korobov, *Number-theoretical methods in approximate analysis*, Fizmatgiz, Moscow, 1963 (in Russian).

[10] R. Kutz, 'Cohen-Macauly rings and ideal theory in rings of invariants of algebraic groups', *Trans. Amer. Math. Soc*, **194** (1974), 115–129.

[11] G. Laumon, 'Exponential sums and l-adic cohomology: A survey', *Israel J. Math.*, **120** (2000), 225–257.

[12] W. Luo, 'Rational points on complete intersections over $\mathbb{F}_p$', *Internat. Math. Res. Notices*, **1999** (1999), 901–907.

[13] K. Morrison, 'Integer sequences and matrices over finite fields', *J. Integer Sequences*, **9** (2006), Article 06.2.1.

[14] H. Niederreiter, 'Quasi-Monte Carlo methods and pseudo-random numbers', *Bull. Amer. Math. Soc.*, **84** (1978), 957–1041.

[15] H. Niederreiter, *Random number generation and Quasi–Monte Carlo methods*, SIAM Press, 1992.

[16] A. Rittatore and W. F. Santos, *Actions and invariants of algebraic groups*, Monographs and Textbooks in Pure and Applied Mathematics, vol. 269, Chapman & Hall/CRC, 2005.

[17] I. Rivin, 'Walks on groups, counting reducible matrices, polynomials, and surface and free group automorphisms', *Preprint*, 2006.

[18] C. Roettger, 'Counting invertible matrices and uniform distribution', *J. Théorie Nombres Bordeaux*, **17** (2005), 301–322.

[19] I. E. Shparlinski, 'Polynomials of given height in finite fields', *Math. USSR-Sb.*, **63** (1989), 247–255.

[20] I. E. Shparlinski, 'Polynomials of given height in finite fields', *Math. USSR-Sb.*, **71** (1992), 41–50.

[21] I. E. Shparlinski, 'Distribution of inverses and multiples of small integers and the Sato–Tate conjecture on average', *Preprint*, 2006.

[22] I. E. Shparlinski and A. N. Skorobogatov, 'Exponential sums and rational points on complete intersections', *Mathematika*, **37** (1990), 201–208.

[23] A. N. Skorobogatov, 'Exponential sums, the geometry of hyperplane sections, and some Diophantine problems', *Israel J. Math.*, **80** (1992), 359–379.