Available online at www.sciencedirect.com

SCIENCE DIRECT®

C. R. Acad. Sci. Paris, Ser. I 343 (2006) 155–159

COMPTES RENDUS MATHEMATIQUE

http://france.elsevier.com/direct/CRASS1/

Number Theory

Sieving and expanders ☆

Jean Bourgain [a], Alex Gamburd [a,b], Peter Sarnak [a,c]

[a] *School of Mathematics, Institute for Advanced Study, Princeton, NJ 08540, USA*
[b] *Department of Mathematics, University of California, Santa Cruz, USA*
[c] *Department of Mathematics, Princeton University, USA*

Received and accepted 29 May 2006

Presented by Jean Bourgain

Abstract

Let V be an orbit in $\mathbb{Z}^n$ of a finitely generated subgroup Λ of $\mathrm{GL}_n(\mathbb{Z})$ whose Zariski closure $\mathrm{Zcl}(\Lambda)$ is suitably large (e.g. isomorphic to SL_2). We develop a Brun combinatorial sieve for estimating the number of points on V for which a fixed set of integral polynomials take prime or almost prime values. A crucial role is played by the expansion property of the 'congruence graphs' that we associate with V. This expansion property is established when $\mathrm{Zcl}(\Lambda) = \mathrm{SL}_2$. ***To cite this article: J. Bourgain et al., C. R. Acad. Sci. Paris, Ser. I 343 (2006).***

Résumé

Cribles et expanseurs. Soit V l'orbite dans $\mathbb{Z}^n$ d'un sous-groupe finiment engendré de $\mathrm{GL}_n(\mathbb{Z})$ don't l'adhérence dans la topologie de Zariski est suffisament grande (p.e. est isomorphe à SL_2). Nous developpons une crible combinatoire de Brun a fin d'estimer le nombre de points de V pour lesquels un system de polynômes donnés prennent des valeurs premières ou presque premières. Des propriétés d'expansion de certain « graphes de congruence » y jouent un rôle crucial, qu'on établi dans le cas $\mathrm{Zcl}(\Lambda) = \mathrm{SL}_2$. ***Pour citer cet article : J. Bourgain et al., C. R. Acad. Sci. Paris, Ser. I 343 (2006).***

Version française abrégée

Le probleme general abordé dans cette Note est le suivant. Soit Λ le sous-groupe de $\mathrm{GL}(n, \mathbb{Z})$ engendré par $A_1, \dots, A_\nu$ et $V = \Lambda b$ l'orbite d'un point $b \in \mathbb{Z}^n$ sous Λ. Soient $f_1, \dots, f_t$ des polynómes en $x \in \mathbb{Z}^n$ a coefficients entiers et prennant un nombre infinie de valeurs sur V. On considère des points $x \in V$ tel que tout $f_j(x)$ soit premier ou plutôt r-premier (c. á. d. produit d'au plus r nombres premiers). Dénotons $\mathrm{Zcl}(\Lambda)$ l'adhérence de Λ pour la topologie de Zariski et supposons $\mathrm{Zcl}(\Lambda) \equiv \mathrm{SL}_2$. Nous demonstrons en particulier que il existe $x \in V$ pour lequel chaque $f_j(x)$ est r-premier et $|f_j(x)| > y$. l'Approche combine des variantes des cribles de Brun–Selberg et de nouvaux resultats sur les expanseurs dans $\mathrm{SL}_2(\mathbb{Z}/q\mathbb{Z})$ qui genéralisant ceux obtenus dans [2] pour q premier.

☆ The first author was supported in part by NSF grant DMS-0322370. The second author was supported in part by NSF grant DMS-0111298 and DMS-0501245. The third author was supported in part by Oscar Veblen Fund (IAS) and the NSF.

E-mail addresses: bourgain@math.ias.edu (J. Bourgain), agamburd@ucsc.edu (A. Gamburd), sarnak@math.princeton.edu (P. Sarnak).

1631-073X/$ – see front matter
doi:10.1016/j.crma.2006.05.023

1. Statement of results

We denote by Zcl the Zariski closure of subsets in affine k-dimensional space $\mathbb{A}^k$ and by P^k the set of all $x = (x_1, \dots, x_k)$ in $\mathbb{A}^k$ such that x_j or $-x_j$ is prime for each j. Dirichlet's Theorem on primes in progressions, as well as the Hardy–Littlewood k-tuple Conjectures [9] can be formulated as the following local-to-global group theoretic statement:

Conjecture 1. *Let Λ be a subgroup of $\mathbb{Z}^k$ whose projection on each coordinate is not zero. Given b in $\mathbb{Z}^k$ let $V = \Lambda + b$ be the corresponding orbit of Λ. Then*

$$\mathrm{Zcl}\big(V \cap P^k\big) = \mathrm{Zcl}(V)$$

iff there are no local congruence obstructions (that is, given $q > 1$, there is $x \in V$ such that $x_1 x_2 \dots x_k \in (\mathbb{Z}/q\mathbb{Z})^*$).

The local obstructions are easily checked and involve only finitely many q. For $k = 1$ Conjecture 1 is essentially Dirichlet's Theorem. For $k > 1$ one can use the combinatorial sieve [8,11] to show that Conjecture 1 is true if we replace the primes by r-almost primes (i.e. numbers which are products of at most r primes) where $r = r(k)$. Using the same techniques one can also give sharp upper bounds (up to a multiplicative factor) for $|V \cap P^k \cap B_X|$, where B_X is a ball of radius X in $\mathbb{A}^k$, as X goes to infinity. For a non-degenerate rank two subgroup Λ in $\mathbb{Z}^3$, Conjecture 1 can be proven using Vinogradov's methods [24], while very recently Green and Tao [7] proved Conjecture 1 for non-degenerate rank two subgroups Λ in $\mathbb{Z}^4$.

The above formulation of Conjecture 1 suggests various non-Abelian versions, of which the simplest is the following:

Conjecture 2. *Let Λ be a non-elementary subgroup of $\mathrm{SL}_2(\mathbb{Z})$ (equivalently, $\mathrm{Zcl}(\Lambda) = \mathrm{SL}_2$), b a primitive point in $\mathbb{Z}^2$ and $V = \Lambda b$ the corresponding orbit. Then*

$$\mathrm{Zcl}\big(V \cap P^2\big) = \mathrm{Zcl}(V)\big(= \mathbb{A}^2\big)$$

iff there are no local congruence obstructions.

The non-elementary condition is necessary. We must clearly avoid finite subgroups but also Conjecture 2 is false for cyclic subgroups. For example, if Λ is generated by $\left(\begin{smallmatrix} 7 & 6 \\ 8 & 7 \end{smallmatrix}\right)$ and $b = \left[\begin{smallmatrix} 1 \\ 1 \end{smallmatrix}\right]$, then there are no local obstructions, but V is contained in $\{(x, y)\colon\ 4x^2 - 3y^2 = 1\}$, from which it is clear that y cannot be prime and hence $V \cap P^2$ is empty. The formulation of the higher dimensional versions of Conjecture 2, as well as the generalization to this non-Abelian setting of Schinzel's hypothesis H [20] is more involved and we leave it to the long version of this paper [3]. Our aim here is to outline the key ingredients needed to develop a combinatorial sieve in this non-Abelian context and to apply it to establish versions of these conjectures with primes replaced by almost primes.

Theorem 1. *Let Λ be a subgroup of $\mathrm{GL}(n, \mathbb{Z})$ whose Zariski closure is SL_2. Fix $f_1, f_2, \dots, f_t$ in $\mathbb{Z}[x_1, \dots, x_n]$, $b \in \mathbb{Z}^n$ and let $V = \Lambda b$. There is an r, depending on Λ, b and the f's, such that the set*

$$V_{f,r} = \big\{x \in V\colon\ f_j(x) \text{ is an } r\text{-almost prime for each } j\big\}$$

is Zariski dense in $\mathrm{Zcl}(V)$.

Applying Theorem 1 to the case that Λ is a non-elementary subgroup of $\mathrm{SL}_2(\mathbb{Z})$ and $f_j(x) = x_j$, $j = 1, 2$, yields an almost prime version of Conjecture 2. The proof of Theorem 1 yields an effective, though very poor, dependence for r on V and the f's. In order to get a better and explicit dependence, or to estimate from above the number of x's for which the $f_j(x)$ are prime, it is best to use an Archimedean norm to order the elements of V. For this analysis we suppose that Λ is a subgroup of $\mathrm{SL}_2(\mathbb{Z})$ and that the action is the standard one on the two by two integer matrices by multiplication on the left, and we consider the orbit V of I (the identity matrix) under Λ. Denote by $|x|$ the norm $(\sum_{i,j} x_{ij}^2)^{1/2}$, where $x = \left(\begin{smallmatrix} x_{11} & x_{12} \\ x_{21} & x_{22} \end{smallmatrix}\right)$. Set $N_\Lambda(y) = |\{x \in \Lambda\colon\ |x| \leqslant y\}|$ and let $\delta(\Lambda)$ be the Hausdorff dimension of the limit set of an orbit $\Lambda z \subset \mathbb{H} \cup \{\infty\} \cup \mathbb{R}$, where $\mathbb{H}$ is the hyperbolic plane, $z \in \mathbb{H}$ and Λ acts by linear fractional transformations. If $\delta(\Lambda) > \frac{1}{2}$ then it is known [12] that $N_\Lambda(y) \sim c_\Lambda y^{2\delta(\Lambda)}$, as $y \to \infty$. Let $f_1, f_2, \dots, f_t$ be integral polynomials in x_1, x_2, x_3, x_4, which when reduced in coordinate ring $\overline{\mathbb{Q}}[x_1, x_2, x_3, x_4]/\langle x_1x_4 - x_2x_3 - 1\rangle$ generate distinct prime ideals. This is an independence condition on the f's when restricted to $\mathrm{Zcl}(V)$. Set

$$\pi_{\Lambda,f}(y) = \bigl|\bigl\{x \in \Lambda;\ |x| \leqslant y,\ f_j(x) \text{ is prime for } j = 1, \ldots, t\bigr\}\bigr|.$$

Theorem 2. *Let Λ be a finitely-generated subgroup of* $\mathrm{SL}(2,\mathbb{Z})$ *with $\delta(\Lambda) > \frac{1}{2}$ and assume that $f_1, \ldots, f_t$ satisfy the above independence condition. Then*

$$\overline{\lim_{y\to\infty}} \frac{\pi_{\Lambda,f_1,\ldots,f_t}(y)(\log y)^t}{N_\Lambda(y)} < \infty.$$

If there is a local congruential obstruction to the $f_j(x)$ being prime on V, then the above $\overline{\lim}$ is zero. If not, then a quantitative version (for the Archimedean ordering) of the non-Abelian Schinzel Conjecture [3] asserts that the above limit exists and is not zero. So the upper bound in Theorem 2 is expected to be sharp except for the multiplicative constant.

The proofs of Theorems 1 and 2 rely on certain families of graphs being expanders (see [17] for a definition). In the more general setting of Λ being a group generated by invertible integer coefficient polynomial maps $A_1, A_2, \ldots, A_\nu$ of $\mathbb{Z}^n$ and an orbit $V = \Lambda b$ of b in $\mathbb{Z}^n$ under Λ, we define the associated 'congruence graphs' as follows: For $q \geqslant 1$ let $V(q)$ be the subset of $(\mathbb{Z}/q\mathbb{Z})^n$ that results from reducing V modulo q. We make this into a 2ν regular graph $\mathcal{G}(V(q); A_1^{\pm1}, \ldots, A_\nu^{\pm1})$ by taking the vertices of the graph to be $V(q)$ and joining x to y with the number of edges equal to the number of B's in $\{A_1^{\pm1}, \ldots, A_\nu^{\pm1}\}$ such that $Bx = y$.

Theorem 3. *Let $\Lambda = \langle A_1, \ldots, A_\nu\rangle \subset \mathrm{GL}(n,\mathbb{Z})$, $V = \Lambda\xi$ and assume that $\mathrm{Zcl}(\Lambda) \cong \mathrm{SL}_2$. Then for $q \geqslant 1$ the graphs $\mathcal{G}(V(q); A_1^{\pm1}, \ldots, A_\nu^{\pm1})$ form an expander family.*

This extends the recent results [2] to this setting and also from q prime to q square-free (thus also providing affirmative answer to Lubotzky's 1–2–3 problem [13] for q square-free). The proof of Theorem 3 builds crucially on the following sum–product estimate, which extends results in [5,4].

Theorem 4. *Let $\delta_1 \geqslant \delta_2 > 0$. Let $q = \prod_{j=1}^J p_j$ be a product of distinct primes. For $q'|q$, let $\pi_{q'}$ denote the projection $\mathbb{Z}/q\mathbb{Z} \to \mathbb{Z}/q'\mathbb{Z}$. Let $A \subset \mathbb{Z}/q\mathbb{Z}$ and assume that*

$$q^{\delta_1} < |A| < q^{1-\delta_1}$$

and

$$\bigl|\pi_{q_1}(A)\bigr| > q_1^{\delta_2} \quad \textit{for all } q_1|q \textit{ with } q_1 > q^{\delta_1/3}.$$

Then

$$|A + A| + |A \cdot A| > q^{\delta_3}|A|$$

where $\delta_3 = \delta_3(\delta_1, \delta_2) > 0$.

For the sieving which uses Archimedean norm (rather than word-length norm used to prove Theorem 1) we need a continuous (non-Euclidean) analogue of Theorem 3 in the form of the appropriate spectral gap result. Here we assume that Λ is a finitely generated subgroup of $\mathrm{SL}(2,\mathbb{Z})$ and $\delta(\Lambda) > \frac{1}{2}$. Let $X_\Lambda = \Lambda\backslash\mathbb{H}$ be the corresponding hyperbolic surface (which is of infinite volume if Λ is of infinite index in $\mathrm{SL}(2,\mathbb{Z})$). The spectrum of the Laplace–Beltrami operator on $L^2(X_\Lambda)$ consists of finite number of points in $[0, \frac{1}{4})$ (see [12]). We denote them by

$$0 \leqslant \lambda_0(\Lambda) < \lambda_1(\Lambda) \leqslant \cdots \leqslant \lambda_{\max}(\Lambda) < \frac{1}{4}.$$

The assumption that $\delta(\Lambda) > \frac{1}{2}$ is equivalent to $\lambda_0(\Lambda) < \frac{1}{4}$ and in this case $\delta(1-\delta) = \lambda_0$ [16].

Theorem 5. *Let Λ be a finitely generated subgroup of* $\mathrm{SL}(2,\mathbb{Z})$ *with* $\delta(\Lambda) > \frac{1}{2}$. *For* $q \geqslant 1$ *let* $\Lambda(q)$ *be the 'congruence' subgroup* $\{x \in \Lambda\colon\ x \equiv I \bmod q\}$. *There is* $\varepsilon = \varepsilon(\Lambda) > 0$ *such that*

$$\lambda_1\big(\Lambda(q)\big) \geqslant \lambda_0\big(\Lambda(q)\big) + \varepsilon,$$

for all square-free $q \geqslant 1$ (*note that* $\lambda_0(\Lambda(q)) = \lambda_0(\Lambda)$).

This gives an infinite volume extension of Selberg's well-known bound for modular surfaces [22]. In [6] an explicit and stronger version of Theorem 5 is proven under the assumption that $\delta(\Lambda) > \frac{5}{6}$. See [18] for the sharpest known bounds towards Selberg's $\frac{1}{4}$ Conjecture as well as bounds towards the Ramanujan Conjectures for more general groups. These have direct application to the problem at hand in the special but interesting case (which we call the algebraic case as opposed to the general combinatorial 'thin orbit' case of this note) that the subgroup Λ is an arithmetic lattice in a semi-simple group G defined over $\mathbb{Q}$, see [15].

We expect that Theorem 1 holds under the general assumption that $\mathrm{Zcl}(\Lambda)$ is semi-simple, connected and simply connected. The only part of the proof that needs to be further developed in order to handle this general case is the combinatorics used to prove Theorem 3 (in particular, extending [10] and [2]).

2. Brief outline of proofs

We begin with Theorem 1. First, using an appropriate adaptation of the argument in [23], we pass to a free subgroup F of Λ, generated by two elements A and B, which is Zariski-dense in $\mathrm{Zcl}(\Lambda)$, and for which $\mathrm{Stab}_F(\xi) = \{1\}$. We order the elements x of F by word length $w(x)$ in the generators A and B. For $R \geqslant 1$ an integer, let

$$N_F(R) = \big|\big\{x \in F\colon\ w(x) \leqslant R\big\}\big| = 4 \cdot 3^{R-1}.$$

By an elementary analysis of the subgroups of $\mathrm{SL}_2(\mathbb{Z}/q\mathbb{Z})$, or, in greater generality by invoking the strong approximation theorem in [14], there is $q_1 = q_1(\Lambda)$ such that the injection of F into $\prod_{(p,q_1)=1} \mathrm{SL}_2(\mathbb{Z}_p)$ is dense. In particular, the projection $F \hookrightarrow \mathrm{SL}_2(\mathbb{Z}/q\mathbb{Z})$ is onto if $(q, q_1) = 1$. Using the expander property (Theorem 3) one shows that for any nonconstant f in $\mathbb{Z}[x_1, x_2, x_3, x_4]/\langle x_1x_4 - x_2x_3 - 1\rangle$ we have

$$\big|\big\{x \in F \mid w(x) \leqslant R,\ f(x) = 0\big\}\big| = \mathrm{O}\big(N_F(R)^{\gamma}\big) \tag{1}$$

for a fixed $\gamma < 1$. For $n \geqslant 1$ set

$$a_n(R) = \big|\big\{x \in F \mid w(x) \leqslant R,\ \big|f_1 \ldots f_t(x)\big| = n\big\}\big|.$$

Again using the expander property it follows that for $d \geqslant 1$ square-free and $(d, q_1) = 1$

$$\sum_{n \equiv 0(d)} a_n(R) = \frac{\beta(d)}{|\mathrm{SL}_2(\mathbb{Z}/d\mathbb{Z})|} N_F(R) + \mathrm{O}\big(N_F(R)^{\gamma}\big), \tag{2}$$

where

$$\beta(d) = \big|\big\{x \in \mathrm{SL}_2(\mathbb{Z}/d\mathbb{Z})\colon\ f_1(x) \ldots f_t(x) \equiv 0 (\mathrm{mod}\ d)\big\}\big|.$$

This allows us to carry out a (lower bound) combinatorial Brun sieve [11] to conclude that in the case that $f_1, \ldots, f_t$ are irreducible and independent we have the following lower bound for the sum over n sieved for primes up to P:

$$S(R, P) = \sum_{(n,P)=1} a_n(R) \gg \frac{N_F(R)}{(\log z)^t},$$

where $P = \prod_{p \leqslant z,\,(p,q_1)=1} p$ and $z = C^R$ for some $C > 1$, C depending only on $F = \langle A, B\rangle$ and $f_1, \ldots, f_t$. Theorem 1 then follows on noting that $a_n(R) = 0$ for $n \geqslant C_1^R$, where C_1 is large constant depending on A and B only, and using (1) to ensure Zariski density.

It is interesting to note the sharp contrast to the more familiar case where V is linear and for which the analogue of (2) with a very small remainder follows from Poisson summation (and no spectral gap property is needed). In the present case (2) (and its Archimedean analogue discussed below) is essentially equivalent to the expander property and the remainder is never small ($\gamma \geqslant \frac{1}{2}$). In this sense the counting of integral points in progressions on non-Abelian orbits or on nonlinear varieties is similar to counting primes in progressions on the line, where again a square root remainder is the best that one can expect.

Theorem 2 is proved in a similar way except that the counting is done with

$$\tilde{a}_n(R) = \sum_{\substack{x \in L:\ |x| < R \\ |f_1(x) \ldots f_t(x)| = n}} 1,$$

or a smoothed weighted version of this sum which for technical purposes is better. One can evaluate $\sum_{n \equiv 0(d)} \tilde{a}_n(R)$ to the same degree of precision as in (2) above by using [12] and the spectral gap result in Theorem 5. In place of lower bound combinatorial sieve we use an upper bound one, or better still the simpler Selberg's Λ^2 sieve [21].

The proof of Theorem 3 is based on exploiting the large symmetry group of the graphs to ensure high multiplicity of eigenvalues, together with an upper bound on the number of closed cycles (an approach initiated in [19] and subsequently applied in [6] and [2]), the new feature being that q is square-free (and prime to q_1). As for the multiplicity bounds that are needed in the proof, we proceed inductively on the number of prime factors of q. The proof of the upper bound follows the approach in [2] and builds crucially on the sum–product estimate in $\mathbb{Z}_q$ for q square-free (Theorem 4), which we prove using analytic tools for general moduli developed in [1]. Armed with Theorem 4, and following the approach in [10] we derive a product theorem in $\mathrm{SL}_2(\mathbb{Z}/q\mathbb{Z})$; proceeding as in [2] we then give suitable convolution estimates in $\mathrm{SL}_2(\mathbb{Z}/q\mathbb{Z})$ and eventually obtain the required upper bound.

Theorem 5 is deduced from Theorem 3 by a geometrical argument involving renormalization by the (positive) ground-state of Laplacian on $\Lambda\backslash\mathbb{H}$ of the various vector-valued test functions on $\mathbb{H}$, which transform under Λ by representations factoring through $\Lambda/\Lambda(q)$.

Complete proofs as well as concrete examples and applications of the theorems above will appear in [3].

References

[1] J. Bourgain, Exponential sum estimates over subgroups of $\mathbb{Z}_q^*$, q arbitrary, J. Analyse, in press.
[2] J. Bourgain, A. Gamburd, Uniform expansion bounds for Cayley graphs of $\mathrm{SL}_2(\mathbb{F}_p)$, preprint, 2005.
[3] J. Bourgain, A. Gamburd, P. Sarnak, Spectral sieving of thin sets, in preparation.
[4] J. Bourgain, A. Glibichuk, S. Konyagin, Estimate for the number of sums and products and for exponential sums in fields of prime order, Proc. London Math. Soc., in press.
[5] J. Bourgain, N. Katz, T. Tao, A sum–product estimate in finite fields and applications, GAFA 14 (2004) 27–57.
[6] A. Gamburd, Spectral gap for infinite index “congruence” subgroups of $\mathrm{SL}_2(\mathbb{Z})$, Israel J. Math. 127 (2002) 157–200.
[7] B. Green, T. Tao, Linear equations in primes, preprint.
[8] H. Halberstam, H. Richert, Sieve Methods, Academic Press, 1974.
[9] G.H. Hardy, J.E. Littlewood, Some problems of ‘Partitio Numerorum’: III. On the expression of a number as a sum of primes, Acta Math. 44 (1922) 1–70.
[10] H. Helfgott, Growth and generation in $\mathrm{SL}_2(\mathbb{Z}/p\mathbb{Z})$, preprint, 2005.
[11] H. Iwaniec, E. Kowalski, Analytic Number Theory, Amer. Math. Soc., 2004.
[12] P.D. Lax, R.S. Phillips, The asymptotic distribution of lattice points in Euclidean and non-Euclidean space, J. Funct. Anal. 46 (1982) 280–350.
[13] A. Lubotzky, Cayley graphs: eigenvalues, expanders and random walks, in: P. Rowbinson (Ed.), Surveys in Combinatorics, in: London Math. Soc. Lecture Note Ser., vol. 218, Cambridge Univ. Press, 1995, pp. 155–189.
[14] C. Matthews, L. Vaserstein, B. Weisfeiler, Congruence properties of Zariski-dense subgroups, Proc. London Math. Soc. 48 (1984) 514–532.
[15] A. Nevo, P. Sarnak, in preparation.
[16] S.J. Patterson, The limit set of a Fuchsian group, Acta Math. 136 (1975) 241–273.
[17] P. Sarnak, What is an expander?, Notices Amer. Math. Soc. 51 (2004) 762–763.
[18] P. Sarnak, Notes on the generalized Ramanujan conjectures, Clay Math. Proc. 4 (2005) 659–685.
[19] P. Sarnak, X. Xue, Bounds for multiplicities of automorphic representations, Duke Math. J. 64 (1991) 207–227.
[20] A. Schinzel, W. Sierpinksi, Sur certaines hypotheses concernant les nombres premiers, Acta Arith. 4 (1958) 185–208.
[21] A. Selberg, On an elementary method in the theory of primes, Norske Vid. Selsk. Forh. 19 (1947) 64–67.
[22] A. Selberg, On the estimation of Fourier coefficients of modular forms, in: Proc. Sympos. Pure Math., vol. VII, Amer. Math. Soc., 1965, pp. 1–15.
[23] J. Tits, Free subgroups in linear groups, J. Algebra 20 (1972) 250–270.
[24] I.M. Vinogradov, Representations of an odd number as a sum of three primes, Dokl. Akad. Nauk SSSR 15 (1937) 291–294.