Counting Primes, Groups and Manifolds

Dorian Goldfeld[1], Alexander Lubotzky[2],
Nikolay Nikolov[3] and László Pyber[4]

October 20, 2004

Addresses:

1. Department of Mathematics, Columbia University, New York, NY 10027, U.S.A.,

2. Einstein Institute of Mathematics, Hebrew University, Jerusalem 91904, Israel,

3. Tata Institute for Fundamental Research, Colaba, Mumbai 400005, India,

4. A. Rényi Institute of Mathematics, Reáltanoda ut. 13-15, H-1053, Budapest, Hungary.

Corresponding author: Alexander Lubotzky, tel +972 2 6584387, e-mail: alexlub@math.huji.ac.il .

Pages: 11 (double spaced).

Wordcount: abstract 150, main text 2200.

PNAS Classification. Physical sciences: Mathematics.

2000 Mathematics Subject Classification 20H05; 22E40

Abstract

Let $\Lambda = \mathrm{SL}_2(\mathbb{Z})$ be the modular group and let $c_n(\Lambda)$ be the number of congruence subgroups of Λ of index at most n. We prove that $\lim\limits_{n\to\infty} \frac{\log c_n(\Lambda)}{(\log n)^2/\log\log n} = \frac{3-2\sqrt{2}}{4}$. The proof is based on the Bombieri-Vinogradov 'Riemann hypothesis on the average' and on the solution of a new type of extremal problem in combinatorial number theory. Similar surprisingly sharp estimates are obtained for the subgroup growth of lattices in higher rank semisimple Lie groups. If G is such a Lie group and Γ is an irreducible lattice of G it turns out that the subgroup growth of Γ is independent of the lattice and depends only on the Lie type of the direct factors of G. It can be calculated easily from the root system. The most general case of this result relies on the Generalized Riemann Hypothesis but many special cases are unconditional. The proofs use techniques from number theory, algebraic groups, finite group theory and combinatorics.

Statement of results: arithmetic groups

Let n be a large integer, Γ a finitely generated group and M a Riemannian manifold. Denote by $\pi(n)$ the number of primes less or equal to n, $s_n(\Gamma)$ is the number of subgroups of Γ of index at most n and $b_n(M)$ is the number of covers of M of degree at most n. The aim of this note is to announce results which show that in some circumstances, these three seemingly unrelated functions are very much connected. This happens, for example, when Γ is an arithmetic group, in which case it is also the fundamental group of a suitable locally symmetric finite volume manifold M. The studies of $s_n(\Gamma)$ and $b_n(M)$ are then almost the same. Moreover, if Γ has the congruence subgroup property then estimating $s_n(\Gamma)$ boils down to counting congruence subgroups of Γ. The latter is intimately related to the classical problem of counting primes. To present our results we need more notation.

Let G be an absolutely simple, connected, simply connected algebraic group defined over a number field k. For a finite subset of valuations of k including all the archimedean ones, let $\mathcal{O}_S$ denote the ring of S-integers of k and set $\Gamma = G(\mathcal{O}_S)$. A subgroup $H \leq \Gamma$ is called a congruence subgroup if there is some ideal $I \lhd \mathcal{O}_S$ such that H contains the kernel of the homomorphism $\Gamma \to G(\mathcal{O}_S/I)$.

Let $c_n(\Gamma)$ denote the number of congruence subgroups of index at most n in Γ. The counting of congruence subgroups in arithmetic groups has already played a role in the proof of one of the main results of the theory of subgroup growth: A finitely generated residually finite group Γ has polynomial subgroup growth (i.e. $s_n(\Gamma) = n^{O(1)}$) if and only if Γ is virtually solvable of finite rank (cf. [**?**] and the references therein). That theorem required only a weak lower bound on the number congruence subgroups. In [**?**] Lubotzky proved a more precise result: there exist numbers a, b depending on G, k and S, such that*

$$n^{\frac{a \log n}{\log \log n}} \leq c_n(\Gamma) \leq n^{\frac{b \log n}{\log \log n}},$$

* The lower bound depended on GRH at the time but was made unconditional in [**?**]

and, moreover the sequence $s_n(\Gamma)$ has much faster growth (at least $n^{\log n}$) if the congruence subgroup property fails for G. Below we determine the precise rate of growth of $c_n(\Gamma)$. (All logarithms are in base e.)

Let X be the Dynkin diagram of the split form of G (e.g. $X = A_{n-1}$ if $G = \mathrm{SU}_n$). Let h be the Coxeter number of the root system Φ corresponding to X (it is the order of the Coxeter element of the Weyl group of X). Then $h = \frac{|\Phi|}{l}$ where $l = \mathrm{rank}_{\mathbb{C}}(G) = \mathrm{rank}(X)$, and for later use define $R := h/2$. Let

$$\gamma(G) = \frac{(\sqrt{h(h+2)} - h)^2}{4h^2}.$$

Let GRH denote the Generalized Riemann Hypothesis for Artin-Hecke L-functions of number fields as stated in [?]. The GRH implies in particular:

Let k be a Galois number field of degree d over the rationals and let q be a prime such that the cyclotomic field of q-th roots of unity is disjoint from k. Denote by $\pi_k(x,q)$ the number of primes p with $p \leq x,\ p \equiv 1(\mod q)$ and p splits completely at k. Then

$$\left|\pi_k(x,q) - \frac{x}{d\phi(q)\log x}\right| < Cx^{\frac{1}{2}} \log x \log q$$

for some constant $C = C(k) > 0$ depending only on k (a more precise bound is given in [?]).

The lower bound for the limit in the following Theorem was proved in [?] and the upper bound in [?]:

Theorem 1 *Let G, Γ and $\gamma(G)$ be as defined above. Assuming GRH we have*

$$\lim_{n\to\infty} \frac{\log c_n(\Gamma)}{(\log n)^2/\log\log n} = \gamma(G),$$

and moreover, this result is unconditional if G is of inner type (e.g. G splits) and k is either an abelian extension of $\mathbb{Q}$ or a Galois extension of degree less than 42.

An interesting aspect of this theorem is not only that the limit exists but that it is completely independent of k and S, and depends only on G. While the independence on S is a minor point and can be proved directly, the only way we know to prove the independence on k is by applying the whole machinery of the proof.

In [?] the crucial special case of $\Gamma = \mathrm{SL}_2(\mathcal{O}_S)$ is proved in full. There we have $\gamma(\mathrm{SL}_2) = \frac{1}{4}(3-2\sqrt{2})$. The lower bound follows using the Bombieri-Vinogradov Theorem [?] and the upper bound by a massive new combinatorial analysis.

Lattices

Let H be a connected *characteristic 0* semisimple group. By this we mean that $H = \prod_{i=1}^{r} G_i(K_i)$ where for each i, K_i is a local field of characteristic 0 and G_i is a connected simple algebraic group over K_i. We assume throughout that none of the factors $G_i(K_i)$ is compact (so that $\mathrm{rank}_{K_i}(G_i) \geq 1$). Let Γ be an irreducible lattice of H, i.e. for every infinite normal subgroup N of H the image of Γ in H/N is dense there.

Assume now that

$$\mathrm{rank}(H) := \sum_{i=1}^{r} \mathrm{rank}_{K_i}(G_i) \geq 2.$$

By Margulis' Arithmeticity Theorem ([?]) every irreducible lattice Γ in H is arithmetic. Also the split forms of the factors G_i of H are necessarily of the same type and we set $\gamma(H) := \gamma(G_i)$.

Moreover, a famous conjecture of Serre ([?]) asserts that such a group Γ has the (modified) congruence subgroup property. It has been proved in many cases. This enables us to prove:

Theorem 2 *Assuming GRH and Serre's conjecture, then for every non-compact higher rank characteristic 0 semisimple group H and every irreducible lattice Γ in H the limit*

$$\lim_{n\to\infty} \frac{\log s_n(\Gamma)}{(\log n)^2/\log\log n}$$

exists and equals $\gamma(H)$, i.e. it is independent of the lattice Γ.

Moreover the above holds unconditionally if H is a simple connected Lie group not locally isomorphic to $D_4(\mathbb{C})$ and Γ is a non-uniform lattice in H (i.e. H/Γ is non-compact).

Theorem 2 shows, in particular, some algebraic similarity between different lattices Γ in the same Lie group G. This is an addition to other results in the theory e.g. Furstenberg's theorem showing that the boundaries of all such Γ's are the same or Margulis super-rigidity, which shows that the finite dimensional representation theory of the different Γ's in the same G are similar. (cf [**?**] and the references therein).

We point out the following geometric reformulation of the special case:

Theorem 3 *Let H be a simple connected Lie group of $\mathbb{R}$-rank ≥ 2 which is not locally isomorphic to $D_4(\mathbb{C})$. Put $X = H/K$ where K is a maximal compact subgroup of H. Let M be a finite volume non-compact manifold covered by X and let $b_n(M)$ be the number of covers of M of degree at most n. Then $\lim\limits_{n\to\infty} \frac{\log b_n(M)}{(\log n)^2/\log\log n}$ exists, equals $\gamma(H)$ and is independent of M.*

It is interesting to compare Theorems 2 and 3 with the results of Liebeck and Shalev [**?**] and T. W. Müller, J.-C. Puchta, (*Character theory of symmetric groups, subgroup growth of Fuchsian groups and random walks*, to appear): If $H = \mathrm{SL}_2(\mathbb{R})$ and Γ is a lattice in H then $\lim\limits_{n\to\infty} \frac{\log s_n(\Gamma)}{\log n!} = -\chi(\Gamma)$, where χ is the Euler characteristic.

We finally mention a conjecture and a question: Let X be the symmetric space associated with a simple Lie group H as in Theorem 3. Denote by $m_n(X)$ the number of manifolds covered by X of volume at most n. By a well known result of Wang [**?**], this number is finite unless H is locally isomorphic to $SL_2(\mathbb{R})$ or $SL_2(\mathbb{C})$.

Conjecture. If $\mathbb{R}$-rank$(H) \geq 2$ then

$$\lim_{n\to\infty} \frac{\log m_n(X)}{(\log n)^2/\log\log n} = \gamma(H).$$

Question: Estimate $m_n(X)$ for the case of H having $\mathbb{R}$-rank equal to one. For $H = \mathrm{SO}(n,1)$ the results of [**?**] suggest that $\lim\limits_{n\to\infty} \frac{\log m_n(H)}{\log n!}$ may exist, but we do not have any clue what it could be.

Proofs: the lower bound

We shall illustrate the main idea of the proof with $\Gamma = \mathrm{SL}_d(\mathbb{Z})$ and refer to [**?**] for the full details.

Choose any $\rho \in (0, \frac{1}{2})$. For $x >> 0$ and a prime $q < x$ let $P(x, q)$ be the set of primes $p \leq x$ such that $p \equiv 1 \mod q$. Let $L(x, q) = |P(x, q)|$ and $M(x, q) = \sum_{p \in P(x,q)} \log p$. Then the Bombieri-Vinogradov Theorem [**?**] ensures the existence of a prime $q \in (\frac{x^\rho}{\log x}, x^\rho)$ such that

$$L(x,q) = \frac{x}{\phi(q)\log x} + O\left(\frac{x}{\phi(q)(\log x)^2}\right); \quad M(x,q) = \frac{x}{\phi(q)} + O\left(\frac{x}{\phi(q)(\log x)^2}\right).$$

Put $L := L(x, q)$ and $M := M(x, q)$.

By strong approximation (cf. [**?**], Window 9) Γ maps onto $G_P := \prod_{p \in P(x,q)} \mathrm{SL}_d(\mathbb{F}_p)$. Let $B(p)$ be the subgroup of upper triangular matrices of $\mathrm{SL}_d(\mathbb{F}_p)$ and set

$$B_P := \prod_{p \in P(x,q)} B(p).$$

The group B_P maps onto the diagonal $\prod_p (\mathbb{F}_p^*)^{d-1}$ which in turn maps onto $\mathbb{F}_q^{(d-1)L}$. For fixed $\sigma \in (0, 1) \cap \frac{1}{L(d-1)}\mathbb{N}$ the latter vector space has about $q^{\sigma(1-\sigma)(d-1)^2L^2}$ subgroups of index $q^{\sigma(d-1)L}$ (see Proposition 1.5.2 in [**?**]), each giving rise to a subgroup of index $n = [G_P : B_P]q^{\sigma(d-1)L}$ in Γ. Now $\log[G_P : B_P] \sim d(d-1)M/2$ as $x \to \infty$ and after some algebraic manipulations we obtain that for this chosen value of n

$$\frac{\log c_n(\Gamma)}{(\log n)^2/\log\log n} \geq \frac{\sigma(1-\sigma)\rho(1-\rho)}{(\sigma\rho + R)^2} - o(1), \quad (x \to \infty)$$

where in our case $R = d/2$. As shown in [**?**] §3 the maximum value of the above expression for $\sigma, \rho \in (0, 1)$ is precisely $\gamma(G) = \frac{(\sqrt{R(R+1)}-R)^2}{4R^2}$ and is achieved for $\sigma_0 = \rho_0 = \sqrt{R(R+1)} - R$. By taking x sufficiently large we can choose $\sigma \in (0, 1) \cap \frac{1}{L(d-1)}\mathbb{N}$ to be arbitrarily close to σ_0, and take $\rho = \rho_0$. This proves the lower bound.

The reason for invoking the GRH in Theorem **??** is that in the general case we need an equivalent of the Bombieri-Vinogradov theorem for k in place of $\mathbb{Q}$.

The work of M.R. Murty and V.K. Murty [?] gives an analogue of it for number fields but their result is weaker in general. It suffices for our needs when, for example $k/\mathbb{Q}$, is an abelian extension.

The upper bound

The proof of the upper bound in [?] is inspired by the special case solved in [?] and has two parts:

I. A reduction to an extremal problem for abelian groups, and

II. Solving this extremal problem (Theorem **??** below).

Part I:

The subgroup structure of the groups $\mathrm{SL}_2(\mathbb{F}_p)$ is completely known. Using this it is shown in [?] that Theorem **??** for $\mathrm{SL}_2(\mathbb{Z})$ is equivalent to the following extremal result on counting subgroups of abelian groups:

Let C_m denote the cyclic group of order m. For all pairs $\mathcal{P}_-$ and $\mathcal{P}_+$ of disjoint sets of primes, let

$$f(n) := \max \left\{ s_r(X) \;\middle|\; X = \prod_{p \in \mathcal{P}_-} C_{p-1} \times \prod_{p \in \mathcal{P}_+} C_{p+1} \right\},$$

where the maximum is taken over all sets $\mathcal{P}_-, \mathcal{P}_+$ and $r \in \mathbb{N}$ such that $n \geq r \prod_{p \in \mathcal{P}} p$, (here $\mathcal{P} = \mathcal{P}_- \cup \mathcal{P}_+$).

Theorem 4 *We have*

$$\limsup_{n\to\infty} \frac{\log c_n(\mathrm{SL}_2(\mathbb{Z}))}{(\log n)^2/\log\log n} = \limsup_{n\to\infty} \frac{\log f(n)}{(\log n)^2/\log\log n}.$$

By contrast there is no such precise description of the subgroup structure even for $\mathrm{SL}_n(\mathbb{F}_p)$. Still, surprisingly, the proof of the general upper bound reduces to a similar extremal problem for abelian groups using some ideas of [?], [?] and the following Theorem which is the main new ingredient in [?].

Let $X(\mathbb{F}_q)$ be a finite quasisimple group of Lie type X over the finite field $\mathbb{F}_q$ of characteristic $p > 3$. For a subgroup H of $X(\mathbb{F}_q)$ define

$$t(H) = \frac{\log[X(\mathbb{F}_q) : H]}{\log |H^{\diamond}|},$$

where $H^{\diamondsuit}$ denotes the maximal abelian quotient of H whose order is coprime to p. Set $t(H) = \infty$ if $|H^{\diamondsuit}| = 1$.

Recall that $R = R(X) = h/2$ where h is the Coxeter number of the root system of the **split** Lie type corresponding to X.

Theorem 5 *Given the Lie type X then*

$$\liminf_{q\to\infty} \ \min\{t(H) \mid \quad H \leq X(\mathbb{F}_q)\ \} \geq R.$$

The proof of this theorem does not depend on the classification of the finite simple groups, we use instead the work of Larsen and Pink [**?**] (which is a classification-free version of a result of Weisfeiler [**?**]), and Liebeck, Saxl and Seitz [**?**] (the latter for groups of exceptional type).

Part II:

Once Part I is proved, the argument reduces to an extremal problem on abelian groups:

Theorem 6 *Let d and R be fixed positive numbers. Suppose $A = C_{x_1} \times C_{x_2} \times \cdots \times C_{x_t}$ is an abelian group such that the orders $x_1, x_2, ..., x_t$ of its cyclic factors do not repeat more than d times each. Suppose that $r|A|^R \leq n$ for some positive integers r and n. Then as n, r tend to infinity we have*

$$s_r(A) \leq n^{(\gamma+o(1))\frac{\log n}{\log\log n}},$$

where $\gamma = \frac{(\sqrt{R(R+1)}-R)^2}{4R^2}$.

The starting point of the proof of this theorem in [**?**] is a well-known formula for counting subgroups of finite abelian groups (see [**?**]). We refer the reader to [**?**] for the details which are too complicated to be given here.

Acknowledgments

In their work the authors were supported by grants from the National Science Foundation (Goldfeld and Lubotzky), the Israel Science Foundation and the US-Israel Binational Science Foundation (Lubotzky) and Hungarian National

Foundation for Scientific Research, Grant T037846 (Pyber). While this research was carried out Nikolov held a Golda-Meir Postdoctoral Fellowship at the Hebrew University of Jerusalem. The authors would also like to take this opportunity to thank H. Bass for several helpful comments.

References

[1] A. Lubotzky, D. Segal, *Subgroup growth*, Progress in Mathematics 212, Birkäuser, Boston, 2003.

[2] A. Lubotzky, Subgroup growth and congruence subgroups, *Inv. Math. 119 (1995), 267-295.*

[3] D. Goldfeld, A. Lubotzky, L. Pyber, Counting congruence subgroups, *Acta Math., in press.*

[4] A. Weil, *Sur les "formules explicites" de la théorie des nombres premiers*, Oeuvres Scientifiques, Springer-Verlag, Volume II, 48 - 61.

[5] M. R. Murty, V. K. Murty, N. Saradha, Modular forms and the Chebotarev density theorem. *Amer. J. Math. 110 (1988), no. 2, 253–281.*

[6] A. Lubotzky, N. Nikolov, Subgroup growth of lattices in semisimple Lie groups, *Acta Math., in press.*

[7] E. Bombieri, On the large sieve, *Mathematika 12 (1965), 201-225.*

[8] G. Margulis, *Discrete Subgroups of Semisimple Lie Groups*, Ergebnisse der Math. 17, Springer-Verlag, 1991.

[9] J-P. Serre, Le problème des groupes de congruence pour SL_2, *Ann. of Math. (2) 92, (1970), 489-527.*

[10] M.W. Liebeck, A. Shalev, Fuchsian groups, coverings of Riemann surfaces, subgroup growth, random quotients and random walks, *J. Algebra 276 (2004), no. 2, 552–601.*

[11] H. C. Wang, Topics on totally discontinuous groups, *Symmetric Spaces (W. Boothby, G. Weiss, eds.), M. Dekker (1972), 460–487.*

[12] M. Burger, T. Gelander, A. Lubotzky, S. Mozes, Counting hyperbolic manifolds, *Geometric and Functional Analysis (GAFA), Vol. 12 (2002) 1161-1173.*

[13] M. R. Murty, V. K. Murty, A variant of the Bombieri-Vinogradov theorem, *Canad. Math. Soc. Conference Proceedings 7 (1987), 243-272.*

[14] M. Liebeck, L. Pyber. Finite linear groups and bounded generation, *Duke Math. J. 107 (2001), no. 1, 159-171.*

[15] M. Larsen, R. Pink, Finite subgroups of algebraic groups, *J. Amer. Math. Soc., in press.*

[16] B. Weisfeiler, Post-classification version of Jordan's theorem on finite linear groups, *Proc. Nat. Acad. Sci U.S.A. 81 (1984), 5278-5279.*

[17] M. Liebeck, J. Saxl, G. Seitz, Subgroups of maximal rank in finite exceptional groups of Lie type, *Proc. London Math. Soc.(3) 65 (1992), 297-325.*

[18] L. M. Butler, A unimodality result in the enumeration of subgroups of a finite abelian group, *Proc. Amer. Math. Soc. 101 (1987), 771-775.*