ACTA ARITHMETICA
Online First version

The large sieve revisited

by

M. Ram Murty (Kingston, ON)

To Henryk Iwaniec, on the occasion of his 75th birthday

Abstract. We interpret the large sieve inequality as essentally a character-theoretic inequality on the Prüfer group $\widehat{\mathbb{Z}}$. This perspective allows us to formulate a general "profinite sieve".

1. Introduction. The general sieve problem can be stated as follows. If $\mathscr{A}$ is a set of objects, $\mathscr{P}$ an index set of primes such that for each $p \in \mathscr{P}$ we have a subset $\mathscr{A}_p$ of $\mathscr{A}$, then determine the size of the set

$$S(\mathscr{A}, \mathscr{P}) := \mathscr{A} \setminus \bigcup_{p \in \mathscr{P}} \mathscr{A}_p.$$

In other words, $S(\mathscr{A}, \mathscr{P})$ is the set of elements of $\mathscr{A}$ that do not belong to any of the $\mathscr{A}_p$ with $p \in \mathscr{P}$. Of course, if $\mathscr{A}$ is finite, the classical inclusion-exclusion principle gives an explicit formula for this quantity as follows. For each subset I of $\mathscr{P}$, we define

$$\mathscr{A}_I := \bigcap_{p \in I} \mathscr{A}_p$$

with the understanding that $\mathscr{A}_\emptyset = \mathscr{A}$ when I is the empty set $\emptyset$. Then

$$|S(\mathscr{A}, \mathscr{P})| = \sum_{I \subseteq \mathscr{P}} (-1)^{|I|} |\mathscr{A}_I|.$$

In the context of number theory, one often has for $\mathscr{A}$ a finite set of integers which can be viewed as a subset of elements of the additive cyclic group of integers $\mathbb{Z}$. Many sieve inequalities such as Brun's sieve and Selberg's sieve thus exploit divisibility properties of the integers to derive upper and lower bounds for $S(\mathscr{A}, \mathscr{P})$. By contrast, the large sieve is really an inequality

2020 *Mathematics Subject Classification*: Primary 11N35; Secondary 11R32.
Key words and phrases: large sieve, profinite groups.
Received 4 July 2023; revised 22 October 2023.
Published online *.

involving characters of finite order of the group $\mathbb{Z}$ and thus, at first glance, does not look like a sieve inequality. Indeed, the large sieve inequality [7] is often stated as follows. For any set of complex numbers a_n with $1 \le n \le N$, we have

$$(1) \qquad \sum_{q \le Q} \sum_{(a,q)=1} \left| \sum_{n=1}^{N} a_n e\left(\frac{an}{q}\right) \right|^2 \le (N + Q^2) \sum_{n=1}^{N} |a_n|^2, \qquad e(t) := e^{2\pi i t}.$$

One then derives some combinatorial inequalities to deduce a traditional sieve inequality from the above via the following inequality. Let A be a set of numbers $\le N$ and suppose for each prime $p \le Q$ that the size of the set $A \pmod p$ is bounded by ν_p. Letting $a_n = 1$ if $n \in A$ and zero otherwise, one first shows that for each squarefree q,

$$\left| \sum_{n=1}^{N} a_n \right|^2 \prod_{p|q} \frac{p - \nu_p}{\nu_p} \le \sum_{(a,q)=1} \left| \sum_{n=1}^{N} a_n e\left(\frac{an}{q}\right) \right|^2.$$

Summing this over $q \le Q$ and using (1) gives

$$|A| \le \frac{N + Q^2}{L(Q)}, \qquad L(Q) = \sum_{q \le Q} \mu^2(q) \prod_{p|q} \frac{p - \nu_p}{\nu_p}.$$

This form of the large sieve is due to Montgomery [6].

One way to view this inequality is to view it as a quantitative version of the Hasse principle. More precisely, we have a finite set of integers A whose size we want to estimate and we do this by piecing together information about the size of its image $(\bmod p)$ for various primes p.

We now revisit the large sieve inequality and place it in "larger" context (no pun intended). We interpret this as essentally a character-theoretic inequality on the Prüfer group $\widehat{\mathbb{Z}}$. This perspective allows us to formulate a general "profinite sieve". It is hoped that this wider perspective will have applications especially to "non-abelian" generalizations of the large sieve. Finally, we point out that Ramaré has developed similar material in his lecture notes [12] (see also [13–15]).

2. Preliminaries on profinite groups. We recall in this section basic facts about profinite groups and refer the reader to [11] for further details. A partially ordered set $(I, \le)$ is said to be a *directed set* if for any two $i, j \in I$ there exists a k such that $i \le k$ and $j \le k$. A *profinite system of groups* over I is a family of groups G_i together with morphisms $f_{ij} : G_j \to G_i$, for $i \le j$,

$$\{G_i, f_{ij} : i, j \in I,\ i \le j\},$$

such that the following diagram commutes for all $i \le j \le k$:

$$G_k \xrightarrow{f_{jk}} G_j \xrightarrow{f_{ij}} G_i, \qquad G_k \xrightarrow{f_{ik}} G_i$$

The projective limit (also called inverse limit), denoted by

$$G = \varprojlim_{i \in I} G_i,$$

is the subset of

$$\prod_{i \in I} G_i \tag{2}$$

consisting of tuples $(x_i)_{i \in I}$ satisfying $f_{ij}(x_j) = x_i$ for $i \leq j$. In other words, G consists of "compatible" tuples of (2).

An important example to consider is the directed set of natural numbers partially ordered by divisibility. If $d \mid n$, we have a natural projection

$$\mathbb{Z}/n\mathbb{Z} \to \mathbb{Z}/d\mathbb{Z},$$

which is the usual reduction map. The projective limit is denoted $\widehat{\mathbb{Z}}$ and often called the *Prüfer group* in the literature.

Another important example is provided by taking powers of a fixed prime p and considering the natural map $\mathbb{Z}/p^{n+1}\mathbb{Z} \to \mathbb{Z}/p^n\mathbb{Z}$. Thus, we have

$$\mathbb{Z}_p = \varprojlim \mathbb{Z}/p^n\mathbb{Z},$$

which is the familiar ring of p-adic integers.

An immediate application of the Chinese remainder theorem gives the isomorphism

$$\widehat{\mathbb{Z}} \simeq \prod_p \mathbb{Z}_p,$$

where the product is over all primes p.

If the G_i are topological groups, then G is also a topological group with the *profinite topology*: a set U is open in G if and only if U contains a coset of a subgroup of finite index. This makes G into a compact Hausdorff space.

In 1955, a nice proof of the infinitude of primes was given by Furstenberg [3] using the profinite topology of $\widehat{\mathbb{Z}}$. It runs as follows. Suppose there are only finitely many primes p. Each $p\mathbb{Z}$ is closed because its complement is

$$(1 + p\mathbb{Z}) \cup \cdots \cup ((p-1) + p\mathbb{Z})$$

and is open. If there are only finitely many primes p, then $\bigcup_p p\mathbb{Z}$ is closed, and its complement, which is $\{\pm 1\}$, is open, a contradiction.

3. Characters of $\mathbb{Z}$. Since the additive group $\mathbb{Z}$ is a cyclic group generated by 1, any character of $\mathbb{Z}$ is completely determined by its value at 1. Thus, all unitary characters are of the form $n \mapsto e(\alpha n)$ where $\alpha \in \mathbb{R}/\mathbb{Z}$. When α is rational, this character has finite order. Otherwise, it has infinite order. The character $n \mapsto e(an/q)$ with $(a,q) = 1$ has order exactly q. Thus, one can view the outer sum in (1) as a sum over characters of $\mathbb{Z}$ with order less than or equal to Q.

Another viewpoint valid for our discussion is to consider the profinite completion of $\mathbb{Z}$, which we denoted $\widehat{\mathbb{Z}}$ above. This is the inverse limit of the groups $\mathbb{Z}/q\mathbb{Z}$ partially ordered by divisibility. Any subgroup of finite index of $\widehat{\mathbb{Z}}$ is of the form $q\widehat{\mathbb{Z}}$, and the quotient is isomorphic to the group of residue classes modulo q. The profinite topology is such that any continuous character factors through a finite quotient and hence is necessarily of finite order.

4. A general group-theoretic lemma. Suppose $\mathscr{A}$ is a finite set of objects and G is an arbitrary finite group with conjugacy classes denoted by the letter C. We suppose there is a map $f : \mathscr{A} \to G$ given by $n \mapsto \overline{n}$. We consider the sum

$$\sum_{n\in\mathscr{A}} a_n = \sum_C \sum_{\overline{n}\in C} a_n,$$

where $a_n \in \mathbb{C}$ and the outer sum on the right hand side is over all the conjugacy classes C of G. Denoting the inner sum by $Z(G,C)$, let $\nu(G)$ be the number of C for which $Z(G,C) \neq 0$ weighted by $|C|$. Writing

$$\sum_C \sum_{\overline{n}\in C} a_n = \sum_C |C|^{1/2} \sum_{\overline{n}\in C} |C|^{-1/2} a_n,$$

we see by the Cauchy–Schwarz inequality that

$$\Big|\sum_{n\in\mathscr{A}} a_n\Big|^2 \leq \nu(G) \sum_C \frac{1}{|C|} |Z(G,C)|^2. \tag{3}$$

Let us recall the orthogonality relation: for any finite group G, and any $g_C \in C$,

$$\frac{|C|}{|G|} \sum_{\chi\in\widehat{G}} \overline{\chi}(g_C)\chi(a) = \begin{cases} 1 & \text{if } a \in C, \\ 0 & \text{otherwise.} \end{cases}$$

Using this relation, we have

$$Z(G,C) = \frac{|C|}{|G|} \sum_\chi \overline{\chi(g_C)} S(\chi), \quad \text{where} \quad S(\chi) = \sum_n a_n \chi(n),$$

and the first sum is over irreducible characters χ of G. Thus,

$$\sum_C \frac{1}{|C|}|Z(G,C)|^2 = \frac{1}{|G|}\sum_\chi |S(\chi)|^2.$$

Since for the trivial character we have

$$S(1) = \sum_{n\in\mathscr{A}} a_n,$$

it follows from (3) that

$$|S(1)|^2 \le \frac{\nu(G)}{|G|}\Big(\sum_{\chi\neq 1}|S(\chi)|^2 + |S(1)|^2\Big).$$

Therefore, for $\nu(G) < |G|$,

$$|S(1)|^2 \le \frac{\nu(G)}{|G|-\nu(G)}\sum_{\chi\neq 1}|S(\chi)|^2. \tag{4}$$

Suppose we have a set $\mathscr{P}$ of primes, and for each $p\in\mathscr{P}$ a group G_p is given. Suppose further that we have a finite set $\mathscr{A}$ and a map $a\mapsto \overline{a}\in G_p$. The general philosophy of the sieve as outlined in the introduction now takes the form of the question: given the size ν_p of the image of $\mathscr{A}$ in G_p for each $p\in\mathscr{P}$, estimate the size of $\mathscr{A}$.

Let q be squarefree and set $G_q = \prod_{p\mid q} G_p$. We will say a character χ of G_q is *primitive* if χ restricted to each component G_p (with $p\mid q$) is non-trivial. We will use these observations to prove:

THEOREM 4.1. *Let q be squarefree. For each prime $p\mid q$, let $\nu_p = \nu(G_p)$ and suppose that $\nu_p < |G_p|$. Then*

$$|S(1)|^2 \le \Big(\prod_{p\mid q}\frac{\nu_p}{|G_p|-\nu_p}\Big)\sum_{\chi\in\widehat{G}_q}^{*}|S(\chi)|^2,$$

where the star indicates summation over primitive characters of G_q.

Proof. We induct on the number $\omega(q)$ of prime factors of q. If $\omega(q)=1$, we are done by the discussion used to derive (4) preceding the statement of the theorem. In the general case, we observe that $\widehat{G}_q \simeq \prod_{p\mid q}\widehat{G}_p$, and so fixing a prime divisor $p'\mid q$, we have $G_q \simeq G_{p'}\times G_{q/p'}$. Thus, $\widehat{G}_q \simeq \widehat{G}_{p'}\times\widehat{G}_{q/p'}$. Now,

$$\sum_{\chi\in\widehat{G}_q}^{*}|S(\chi)|^2 = \sum_{\psi\in\widehat{G}_{p'}}^{*}\sum_{\lambda\in\widehat{G}_{q/p'}}^{*}|S(\psi\lambda)|^2 = \sum_{\psi\in\widehat{G}_{p'}}^{*}\sum_{\lambda\in\widehat{G}_{q/p'}}^{*}\Big|\sum_n a_n\psi(n)\lambda(n)\Big|^2.$$

By the induction hypothesis, for the inner sum on the right hand side we have

$$\sum_{\lambda\in\widehat{G}_{q/p'}}^{*}\Big|\sum_n a_n\psi(n)\lambda(n)\Big|^2 \geq \Big(\prod_{p|(q/p')}\frac{|G_p|-\nu_p}{\nu_p}\Big)\Big|\sum_n a_n\psi(n)\Big|^2.$$

We sum this over primitive characters ψ of $G_{p'}$ and use the case $\omega(q)=1$ to deduce

$$\begin{aligned}\sum_{\psi\in\widehat{G}_{p'}}^{*}\sum_{\lambda\in\widehat{G}_{q/p'}}^{*}|S(\psi\lambda)|^2 &\geq \Big(\prod_{p|(q/p')}\frac{|G_p|-\nu_p}{\nu_p}\Big)\sum_{\psi\in\widehat{G}_{p'}}^{*}\Big|\sum_n a_n\psi(n)\Big|^2\\ &\geq \Big(\prod_{p|q}\frac{|G_p|-\nu_p}{\nu_p}\Big)\Big|\sum_n a_n\Big|^2,\end{aligned}$$

as desired. ∎

The above theorem can be seen as a non-abelian generalization of a result of Serre for abelian groups (see [17, p. 164]).

If we now let $a_n = 1$ for $n \in \mathscr{A}$ and zero otherwise, we deduce from the above discussion:

THEOREM 4.2. *Suppose that*

$$\sum_{\substack{q\leq Q\\ p|q\Rightarrow p\in\mathscr{P}}}\sum_{\chi\in\widehat{G}_q}^{*}|S(\chi)|^2 \leq \Delta\sum_n |a_n|^2. \tag{5}$$

Then

$$|\mathscr{A}| \leq \Delta\Big(\sum_{\substack{q\leq Q\\ p|q\Rightarrow p\in\mathscr{P}}}\mu^2(q)\prod_{p|q}\frac{|G_p|-\nu_p}{\nu_p}\Big)^{-1}.$$

5. A general setting. As before, $\mathscr{A}$ is a finite set of objects and $\mathscr{P}$ is a finite set of primes. But now, let G be a group such that there is a map $f : \mathscr{A} \to G$ given by $a \mapsto \overline{a}$. For each $p \in \mathscr{P}$, let H_p be a normal maximal subgroup of G of finite index such that $a \in \mathscr{A}_p$ if and only if $\overline{a} \pmod{H_p} \in C_p \subseteq G_p$, where $G_p = G/H_p$ and C_p is a union of conjugacy classes of G_p. Let us write for clarity

$$C_p = \bigcup_i C_p^{(i)},$$

where the $C_p^{(i)}$ are conjugacy classes of G_p.

For each squarefree q composed of primes in $\mathscr{P}$, we let G_q be the direct product of groups $\prod_{p|q} G_p$. For each character χ of G_q, and each conjugacy class C of G_q, we select $g_C \in C$ and let

$$S(\chi) := \sum_{a\in\mathscr{A}}\chi(\overline{a}) = \sum_C Z(q,C)\chi(g_C), \tag{6}$$

where $Z(q, C)$ is the number of elements a of $\mathscr{A}$ with $\overline{a} \in C$ and the sum is over all conjugacy classes of G_q.

For a conjugacy class D of G, recall also that $|D| = [G : C(g_D)]$ where $C(g_D)$ is the centralizer of g_D in G.

Now if D denotes any conjugacy class of G_q, then multiplying both sides of (6) by $\overline{\chi}(g_D)$ and summing over all irreducible characters χ of G_q, by orthogonality of characters we get

$$Z(q, D)|C(g_D)| = \sum_{\chi \in \widehat{G}_q} \overline{\chi}(g_D) S(\chi), \tag{7}$$

where $C(g_D)$ is the centralizer of g_D in G_q. Since $|C(g_D)| = |G_q|/|D|$, we have

$$\frac{|G_q|}{|D|} Z(q, D) = \sum_{\chi \in \widehat{G}_q} \overline{\chi}(g_D) S(\chi).$$

Accordingly, we set

$$T(q, D) := \sum_{\chi \in \widehat{G}_q}^{*} \overline{\chi}(g_D) S(\chi),$$

where again we sum over primitive characters of G_q. We can therefore rewrite (7) as

$$\frac{|G_q|}{|D|} Z(q, D) = \sum_{r|q} T(q/r, D)$$

and by Möbius inversion,

$$|D| T(q, D) = \sum_{r|q} \mu(r) |G_{q/r}| Z(q/r, D).$$

On the other hand,

$$\sum_{D} |D| \, |T(q, D)|^2 = \sum_{\chi, \chi'}^{*} S(\chi) \overline{S(\chi')} \sum_{D} \overline{\chi}(g_D) \chi'(g_D) |D|$$

and the innermost sum is simply the inner product (χ, χ') times $|G_q|$. Thus,

$$\sum_{D} |D| \, |T(q, D)|^2 = |G_q| \sum_{\chi}^{*} |S(\chi)|^2.$$

In other words,

$$\sum_{D} \frac{1}{|D|} \Big| \sum_{r|q} \mu(r) |G_{q/r}| Z(q/r, D) \Big|^2 = |G_q| \sum_{\chi}^{*} |S(\chi)|^2.$$

Thus, the expression (5) can also be interpreted as a "generalized variance" since the above shows

$$\sum_{q \le Q} \frac{1}{|G_q|} \sum_{D} \frac{1}{|D|} \Big| \sum_{r|q} \mu(r) |G_{q/r}| Z(q/r, D) \Big|^2 = \sum_{q \le Q} \sum_{\chi}^{*} |S(\chi)|^2.$$

Indeed, if one were to restrict the summation to primes $p \le Q$, then the left hand side is

$$\sum_{p\le Q} |G_p| \sum_D \left(Z(p,D) - \frac{Z}{|G_p|} \right)^2,$$

where we have assumed that $G_1 = 1$ and $Z = Z(1,1)$.

6. The classical large sieve. We can specialize the previous section to the case $G_q = \mathbb{Z}/q\mathbb{Z}$. The last equation of the previous section simplifies to

$$\frac{1}{q}\sum_{a=1}^{q} \Big| \sum_{r|q} \mu(r)(q/r) Z(q/r, a) \Big|^2 = \sum_{(a,q)=1} |S(a/q)|^2. \tag{8}$$

This identity for q prime first appears in the work of Linnik [5] who initiated the theory of the large sieve. Summing (8) over $q \le Q$ and using the large sieve inequality (1) gives

$$\sum_{q\le Q} \frac{1}{q} \sum_{a=1}^{q} \Big| \sum_{r|q} \mu(r)(q/r) Z(q/r, a) \Big|^2 = \sum_{q\le Q} \sum_{(a,q)=1} |S(a/q)|^2 \le (N + Q^2)N.$$

Linnik applied this to study Vinogradov's conjecture [18] that the least quadratic non-residue modulo p, denoted $n(p)$ with p prime, is $O(p^\epsilon)$ for any $\epsilon > 0$. He showed that the number of primes $p \le x$ for which $n(p) > p^\epsilon$ is $\ll_\epsilon \log\log x$. This is remarkable since he also showed that Vinogradov's conjecture is true on the generalized Riemann hypothesis. Thus, the large sieve implies an unconditional theorem indicating that there are very few exceptions to the conjecture (if any).

7. A duality principle. There is a duality principle that can be used to prove the large sieve inequality.

THEOREM 7.1. *Let c_{ij} be mn complex numbers for $1 \le i \le m$, $1 \le j \le n$. Let λ be a non-negative real number. Then*

$$\sum_{1\le i\le m} \Big| \sum_{1\le j\le n} c_{ij} a_j \Big|^2 \le \lambda \sum_{1\le j\le n} |a_j|^2$$

for any complex numbers $a_1, \dots, a_n$ if and only if

$$\sum_{1\le j\le n} \Big| \sum_{1\le i\le m} c_{ij} b_i \Big|^2 \le \lambda \sum_{1\le i\le m} |b_i|^2$$

for any complex numbers $b_1, \dots, b_m$.

The proof of this is easy and can be reduced to the Cauchy–Schwarz inequality (see for example [1, p. 202]). Thus, by duality, the large sieve is

equivalent to estimating

$$\sum_{n\le N}\Big|\sum_{q\le Q}\sum_{(a,q)=1}c(q,a)e(an/q)\Big|^2.$$

Expanding the square, we obtain

$$\sum_{q,q'\le Q}\sum_{(a,q)=1,\,(a',q')=1}c(q,a)\overline{c(q',a')}\sum_{n\le N}e(n(a/q-a'/q'))$$

and the above sum is bounded by

$$N\sum_{q\le Q}\sum_{(a,q)=1}|c(q,a)|^2+\sum_{q,q'\le Q}\sum_{\substack{(a,q)=(a',q')=1,\\ a/q\ne a'/q'}}|c(q,a)|\,|c(q',a')|\,|a/q-a'/q'|^{-1}$$

By symmetry, the second term on the right hand side is

$$\le\sum_{q\le Q}\sum_{(a,q)=1}|c(q,a)|^2\ll Q^2\log Q.$$

This is off by a factor of $\log Q$. However, with some care, the log factor can be removed. Elliott [2] has discussed the spectral nature of this bound.

8. The profinite sieve. We can thus formulate the problem of the profinite sieve as the problem of estimating

$$\sum_{q\le Q}\sideset{}{^*}\sum_{\chi\in\widehat{G}_q}|S(\chi)|^2.$$

By the duality principle, one reduces this to the study of

$$\sum_{n\le N}\chi(n)\overline{\chi}'(n),$$

for two characters χ,χ' of the profinite group G. This is the Rankin–Selberg type sum [16] and thus, if the associated Dirichlet series has suitable properties, one can estimate this sum in a general way and deduce an inequality applicable in a wider context. At the moment, only if the G_q's are abelian does it seem possible to derive a general inequality, though Iwaniec has considered analogous sums and large sieve type estimates in the context of modular forms [4, Chapter 8].

One particular setting is worthy of further consideration and can be described as follows. Let K be an algebraic number field and $\mathscr{F}$ be a countable family of fields normal and of finite degree over K indexed by primes. The lattice $\mathscr{L}$ spanned by $\mathscr{F}$ gives rise to a directed system of fields L_q/K indexed by squarefree numbers q and partially ordered by inclusion. If $G_q=\mathrm{Gal}(L_q/K)$, we get an inverse system of finite groups and $G=\varprojlim G_q$ is a profinite group. The classical Bombieri–Vinogradov theorem can then be

viewed as a theorem about the distribution of Artin symbols corresponding to the family of cyclotomic extensions $\mathbb{Q}(\zeta_q)/\mathbb{Q}$ where ζ_q is a primitive qth root of unity. The case of $L_q = \mathbb{Q}(\zeta_q, a^{1/q})$ when a is a natural number which is not a perfect square is particularly interesting since it would have some implications towards the Artin primitive root conjecture.

A modest research program in this direction was initiated in several of the author's joint papers where "non-abelian" variants of the Bombieri–Vinogradov theorem were derived (see for example [9,10]). These variants were targeted towards the study of Euclidean rings.

Acknowledgements. I thank Abhishek Bharadwaj, Kumar Murty, Sunil Naik, Purusottam Rath and the referee for their helpful remarks on an earlier version of this paper.

Research of the author was partially supported by an NSERC Discovery grant.

References

[1] A. C. Cojocaru and M. R. Murty, *An Introduction to Sieve Methods and Their Applications*, London Math. Soc. Student Texts 66, Cambridge Univ. Press, 2006.
[2] P. D. T. A. Elliott, *On inequalities of large sieve type*, Acta Arith. 18 (1971), 405–422.
[3] H. Furstenberg, *On the infinitude of primes*, Amer. Math. Monthly 62 (1955), 353.
[4] H. Iwaniec, *Spectral Methods of Automorphic Forms*, 2nd ed., Grad. Stud. Math. 53, Amer. Math. Soc., 2002.
[5] Yu. V. Linnik, *The large sieve*, C. R. (Dokl.) Acad. Sci. URSS (N.S.) 30 (1941), 292–294.
[6] H. L. Montgomery, *A note on the large sieve*, J. London Math. Soc. 43 (1968), 93–98.
[7] H. L. Montgomery, *The analytic principle of the large sieve*, Bull. Amer. Math. Soc. 84 (1978), 547–567.
[8] M. R. Murty, *Problems in Analytic Number Theory*, 2nd ed., Springer, 2008.
[9] M. R. Murty and V. K. Murty, *A variant of the Bombieri–Vinogradov theorem*, in: Number Theory, CMS Conf. Proc. 7, Amer. Math. Soc., 1987, 243–272.
[10] M. R. Murty and K. Petersen, *A Bombieri–Vinogradov theorem for all number fields*, Trans. Amer. Math. Soc. 365 (2013), 4987–5032.
[11] J. Neukirch, *Class Field Theory*, Springer, 1986.
[12] O. Ramaré, *Arithmetical Aspects of the Large Sieve Inequality*, HRI Lecture Notes 1, Hindustan Book Agency, 2009.
[13] O. Ramaré, *An explicit result of the sum of seven cubes*, Manuscripta Math. 124 (2007), 59–75.
[14] O. Ramaré, *On long κ-tuples with few prime factors*, Proc. London Math. Soc. 104 (2012), 158–196.
[15] O. Ramaré and I. Z. Ruzsa, *Additive properties of dense subsets of sifted sequences*, J. Théor. Nombres Bordeaux 13 (2001), 559–581.
[16] A. Selberg, *Old and new conjectures and results about a class of Dirichlet series*, in: Proc. Amalfi Conf. on Analytic Number Theory (Maiori, 1989), Università di Salerno, 1992, 367–385; reprinted in: A. Selberg, *Collected Papers II*, Springer, 1991, 47–63.

[17] J.-P. Serre, *Lectures on the Mordell–Weil Theorem*, 2nd ed., Aspects Math. E 15, Vieweg, 1990.

[18] I. M. Vinogradov, *On a general theorem concerning the distribution of the residues and non-residues of powers*, Trans. Amer. Math. Soc. 29 (1927), 209–217.

M. Ram Murty
Department of Mathematics and Statistics
Queen's University
Kingston, ON, Canada, K7L 3N6
E-mail: murty@queensu.ca