SIEVING USING DIRICHLET SERIES

M. Ram Murty[1]

1. Introduction.

Given a sequence of natural numbers, $\{a_n\}_{n=1}^{\infty}$, there are at least three methods in analytic number theory to study properties of this sequence. The first is the method of Dirichlet series. One associates the Dirichlet series

$$f(s) = \sum_{n=1}^{\infty} \frac{a_n}{n^s}$$

and tries to obtain analytic (or meromorphic) continuation of the series to a large enough domain. Then, from the analytic properties of $f(s)$, one tries to obtain information on the growth of the coefficients, or the asymptotic properties of the summatory function

$$\sum_{n \leq x} a_n.$$

This can be viewed as the study of the sequence with respect to the usual (or archimedean) absolute value. A second method is via the sieve technique. One maps the sequence mod p as p ranges over a set of primes. Having some information about the images, one tries to infer properties of the original set. A third technique is the p-adic method, where the study is focussed on the divisibility of the sequence with respect to a single prime. One tries to get some p-adic analytic function to interpolate the values of the sequence and in this way study the sequence. This method can be viewed as the study of the sequence with respect to non-archimedean (or p-adic) absolute values. From this perspective, the sieve method stands at the interface of the other two methods.

It is however, not so well-known, that in many problems of a sieve nature, a simple method involving Dirichlet series can be invoked to obtain very precise information about the divisibility properties of a given sequence, especially when we are trying to sieve by a set of primes that can be described by what we call a Chebotarev condition (see the definition below). This

[1]Research partially supported by an NSERC grant.

method invokes a variant of the classical Wiener-Ikehara Tauberian theorem to derive the final asymptotic formula. Thus, the method cannot be deemed "elementary" both in the technical sense and the practical sense. For most applications, even this can be dispensed with and a simple argument using the sieve of Eratosthenes suffices. The purpose of this paper is to first describe how Dirichlet series can be used to obtain sieve estimates for certain types of problems, and second, how the sieve of Eratosthenes can also be used to obtain similar (albeit weaker) estimates.

Our main purpose in this paper is to show that the sieve of Eratosthenes suffices to derive some of the results of [Se]. Our paper was inspired by Serre's study of divisibility of Fourier coefficients of modular forms [Se]. There he applies the method of Dirichlet series to deduce various theorems concerning Fourier coefficients of Hecke eigenforms. A prototype of the theorems proved in [Se] can be described as follows. Let $\tau(n)$ be the Ramanujan τ-function, defined by the generating function

$$\sum_{n=1}^{\infty} \tau(n) q^n = q \prod_{n=1}^{\infty} (1-q^n)^{24}.$$

Fix a prime $\ell > 2$. Then, almost all (in the sense of natural density) of the coefficients $\tau(n)$ are divisible by ℓ. Moreover,

$$\#\{n \leq x : \quad \tau(n) \not\equiv 0 (\bmod \ell)\} \sim \frac{x}{(\log x)^{\alpha(\ell)}}$$

for some $0 < \alpha(\ell) < 1$.

After reviewing the method of Serre [Se] and making note of its virtues and limitations, we describe how the sieve of Eratosthenes can be invoked to get similar results, which are only "weaker" by a "log log x" factor. However, the latter method is more versatile and can be applied to contexts where the Chebotarev condition (or the "Frobenian property" as Serre calls it) may not hold. The last part of the paper deals with applications of the results.

Acknowledgements. I would like to thank Kalyan Chakraborty and Alina Cojocaru for their comments on an earlier version of this paper.

2. The Method of Dirichlet series.

Let $\mathcal{P}$ be a set of primes and let $\overline{\mathcal{P}}$ indicate its complement in the set of primes. One of the basic problems in sieve theory is to count the number of $n \leq x$ which are not divisible by any of the primes in $\mathcal{P}$. In other words, we want to count the numbers $\leq x$ which are composed of primes solely belonging to $\overline{\mathcal{P}}$. This suggests we define the Dirichlet series

$$f(s) = \sum_{n=1}^{\infty} \frac{a_n}{n^s} = \prod_{p \in \overline{\mathcal{P}}} \left(1 - \frac{1}{p^s}\right)^{-1}$$

so that $a_n = 1$ if n is not divisible by any prime of $\mathcal{P}$ and 0 otherwise. We are therefore interested in the summatory function

$$\sum_{n \leq x} a_n$$

which by the familiar Perron formula (see for example, [M, p. 54-57]) can be written as

$$\frac{1}{2\pi i} \int_{2-i\infty}^{2+i\infty} f(s) \frac{x^s}{s} ds.$$

Clearly, $f(s)$ converges absolutely in the region $Re(s) > 1$. Here is the variant of the classical Tauberian theorem that Serre uses.

Theorem 1. *Suppose that we can write*

$$f(s) = \frac{h(s)}{(s-1)^{1-\alpha}}$$

with $h(s)$ holomorphic in the region $Re(s) \geq 1$ and non-zero there. Then,

$$\sum_{n \leq x} a_n \sim \frac{cx}{(\log x)^{\alpha}}$$

with $c = h(1)/\Gamma(1-\alpha)$, where Γ is the usual Gamma function.

We will derive an application of this result which will be useful in some of the results to be derived below. This involves the enumeration of squarefull numbers. Recall that a natural number n is called squarefull if for every prime

$p|n$, we have $p^2|n$. If we let $a_n = 1$ when n is squarefull and 0 otherwise, then it is easy to see that

$$g(s) = \sum_{n=1}^{\infty} \frac{a_n}{n^s} = \prod_p \left(1 + \frac{1}{p^{2s}} + \frac{1}{p^{3s}} + \cdots\right).$$

Notice that the Euler factor is, with $x = p^{-s}$, equal to

$$1 + x^2(1-x)^{-1} = (1-x^2)^{-1}(1+x^3)$$

so that we can write it as

$$\left(1 - \frac{1}{p^{2s}}\right)^{-1} \left(1 + \frac{1}{p^{3s}}\right).$$

We see immediately that

$$g(s) = \zeta(2s)h(s),$$

where $h(s)$ is analytic for $Re(s) > 1/3$, and $\zeta(s)$ denotes the Riemann zeta function. Changing s to $s - 1/2$, we find that

$$\sum_{n=1}^{\infty} \frac{a_n\sqrt{n}}{n^s} = \zeta(2s-1)h(s-1/2).$$

The right hand side is analytic in $Re(s) \geq 1$ apart from a simple pole at $s = 1$. Theorem 1 implies

$$\sum_{n \leq x} a_n\sqrt{n} \sim cx$$

for some non-zero constant c. Partial summation implies

$$\sum_{n \leq x} a_n \sim c_1\sqrt{x}$$

for some non-zero constant c_1. We also deduce that

$$\sum_{n>y}{}' \frac{1}{n} \ll \frac{1}{\sqrt{y}}$$

where the dash on the summation means that we sum over squarefull numbers. This fact, which will be useful below, easily follows by partial integration and we leave it as an exercise.

3. Applications.

We will say that a set of primes $\mathcal{P}$ satisfies the *Chebotarev condition* if there exists a Galois extension $K/\mathbb{Q}$ of finite degree with Galois group G and a subset D of G stable under conjugation such that for all primes p sufficiently large, $p \in \mathcal{P}$ if and only if the Artin symbol $\sigma_p(K/\mathbb{Q}) \in D$. If we let $\beta = |D|/|G|$ then it is easily seen by using the orthogonality relations for Artin L-functions that for $\mathcal{P}$ satisfying the Chebotarev condition,

$$\sum_{p \in \mathcal{P}} \frac{1}{p^s} = \beta \log\left(\frac{1}{s-1}\right) + \theta(s)$$

where $\theta(s)$ is a function regular in $Re(s) \geq 1$. One can apply Theorem 1 with $\alpha = 1 - \beta$ to deduce

$$\sum_{n \leq x} a_n \sim \frac{cx}{(\log x)^{1-\beta}}$$

for some constant $c \neq 0$, where $a_n = 1$ if n is composed of only primes from $\mathcal{P}$ and is zero otherwise.

By considering the product

$$\prod_{p \in \mathcal{P}} \left(1 + \frac{1}{p^s}\right)$$

we see that Theorem 1 can be applied to show that

$$\sum_{n \leq x} \mu^2(n) a_n \sim \frac{c_1 x}{(\log x)^{1-\beta}},$$

where c_1 is a non-zero constant and μ denotes the Möbius function. Thus, the number of squarefree $n \leq x$ composed of prime numbers of $\mathcal{P}$ also has similar asymptotic behaviour.

For example, if we wanted to count the number of natural numbers $\leq x$ which can be written as the sum of two squares, then by elementary number theory, we see that this is a sieve problem. After some reflection, this reduces to the counting of the number of $n \leq x$ which are not divisible by any prime $\equiv 3(\text{ mod } 4)$. This latter set of primes clearly satisfies the Chebotarev condition with $K = \mathbb{Q}(\sqrt{-1})$ whose Galois group is of order two and we may

take D to be the non-identity element. Thus, $\beta = 1/2$ and we deduce that the number of such integers is

$$\sim cx/\sqrt{\log x},$$

for some non-zero constant.

A more striking example can be given with the Euler ϕ-function. Apart from $\phi(1)$ and $\phi(2)$, we note that $\phi(n)$ is always even. If we fix any odd prime ℓ, we can deduce that for almost all n, $\phi(n)$ is divisible by ℓ. Indeed, the set of primes $\not\equiv 1(\bmod \ell)$ satisfies the Chebotarev condition with $K = \mathbb{Q}(\zeta_\ell)$ whose Galois group is isomorphic to $(\mathbb{Z}/\ell\mathbb{Z})^*$ so that we may take for D the non-identity elements of the Galois group. This is because $p \equiv 1(\bmod \ell)$ if and only if p splits completely in K. Therefore, the number of $n \leq x$, which are not divisible by a prime $p \equiv 1(\bmod \ell)$ is by Theorem 1,

$$\sim \frac{cx}{(\log x)^{1/(\ell-1)}}.$$

Therefore, almost all numbers are divisible by a prime $p \equiv 1(\bmod \ell)$. This means, for almost all numbers, ℓ divides $\phi(n)$.

The result involving Ramanujan's τ-function follows from a result of Deligne [D] who showed the existence of an ℓ-adic representation

$$\rho_\ell : \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \to GL_2(\mathbb{Z}_\ell)$$

such that

$$\mathrm{Tr}\ \rho_\ell(\sigma_p) = \tau(p), \quad \det\ \rho_\ell(\sigma_p) = p^{11}.$$

By considering the "reduction mod ℓ" map, we obtain an extension $K_\ell/\mathbb{Q}$ which is Galois and

$$\mathrm{Tr}\ \rho_\ell(\sigma_p) \equiv \tau(p)(\bmod \ell).$$

Therefore, primes p for which $\ell | \tau(p)$ satisfy a Chebotarev condition. The corresponding β can be calculated from the image of Galois in $GL_2(\mathbb{F}_\ell)$. See [Se] for further details.

An equally striking result is that for algebraic number fields K of finite degree over $\mathbb{Q}$, the Dedekind zeta function

$$\zeta_K(s) = \sum_{\mathfrak{a}} \frac{1}{N(\mathfrak{a})^s} = \sum_{n=1}^{\infty} \frac{a_n}{n^s}$$

has the property that for almost all n, $a_n = 0$ whenever $[K : \mathbb{Q}] > 1$. This is a generalization of the result cited above involving numbers that can be written as the sum of two squares, where in that case $K = \mathbb{Q}(i)$. To see this, let $A(x)$ be the number of $n \leq x$ such that $n = N(\mathfrak{a})$ has a solution. Let $A^*(x)$ be the number of such n which are squarefree. Since any natural number n can be written uniquely as $n = uv$, with $(u, v) = 1$, v squarefull and u squarefree, we see that

$$A(x) = \sum_{v \leq x} A^*(x/v).$$

This sum can be split into two parts, the first being those with $v < z$ and the second with $z \leq v \leq x$. Using the trivial estimate of x/v for $A^*(x/v)$ in the second sum and applying the remark made at the end of the previous section, we find

$$\sum_{z \leq v \leq x} A^*(x/v) \ll \frac{x}{\sqrt{z}}.$$

If we choose $z = \log x$, we find that the contribution from the second sum is $o(x)$ and hence negligible. Now if n is squarefree, a necessary condition for the equation $n = N(\mathfrak{a})$ to have a solution is that $\mathfrak{a}$ is composed of prime ideals of degree 1 over $\mathbb{Q}$. That is, n must be divisible by primes p which have a degree one prime ideal lying above it in K. This is clearly a set of primes satisfying a Chebotarev condition. We can make this more precise. If $\tilde{K}$ denotes the Galois closure of K over $\mathbb{Q}$, and H is the subgroup of $G = \mathrm{Gal}(\tilde{K}/\mathbb{Q})$ that fixes K, then p has a first degree prime ideal in K lying above it if and only if $\sigma_p(\tilde{K}/\mathbb{Q})$ belongs to some conjugate of H. If we let

$$D = \bigcup\nolimits_{g \in G} gHg^{-1}$$

then D is stable under conjugation and we may apply Theorem 1 with $\alpha = 1 - \beta$ with $\beta = |D|/|G|$. It is an elementary exercise in group theory that $0 < \beta < 1$. Indeed, each of the distinct conjugates have the identity element in common and therefore,

$$|D| \leq 1 + (|H| - 1)[G : H] = |G| - [G : H] + 1 < |G|$$

if $[G : H] > 1$ which is the same as saying $K \neq \mathbb{Q}$. By our previous remarks, we deduce

$$A^*(x) \sim \frac{c_1 x}{(\log x)^{1-\beta}}.$$

Inserting this estimate above in the first sum to be considered, we find

$$A(x) \ll \sum_{v<z}{}' \frac{x}{v(\log x)^{1-\beta}}.$$

Since the sum

$$\sum_{v}{}' \frac{1}{v}$$

converges, we find that the total estimate is $o(x)$, as desired.

The above situation is a special case of a more general phenomenon involving Artin L-series. If

$$L(s,\chi) = \sum_{n=1}^{\infty} \frac{a_n}{n^s}$$

is an Artin L-function attached to a Galois extension of $\mathbb{Q}$, such that the set S of elements g belonging to the Galois group with $\chi(g) = 0$ is non-empty, then almost all of the coefficients a_n vanish. The argument to prove this proceeds as above. By the Chebotarev density theorem, the set $\mathcal{P}$ of primes p whose Artin symbol belongs to S has a positive density and hence is Chebotarev. We can proceed as above and deduce that the number of $n \leq x$ such that $a_n \neq 0$ is

$$O\left(\frac{x}{(\log x)^{\delta}}\right)$$

for some $\delta > 0$.

By taking the permutation representation attached to a subgroup H of the Galois group, we see that the Artin L-function is the Dedekind zeta function of the fixed field of H. Indeed, if V is the $\mathbb{C}$-vector space with basis $\{e_{g_iH}\}$, indexed by the cosets of H, the permutation representation $r_{G/H}$ of G attached to the cosets of H is given by the action $g \cdot e_{g_iH} = e_{gg_iH}$ for $g \in G$. It is now straightforward to calculate the character of this representation and we see it is induced from the trivial representation of the subgroup H (see [S, p. 29]). By the invariance of Artin L-series under induction, it follows that the Artin L-series attached to $\chi = \text{tr } r_{G/H}$ is equal to the Dedekind zeta function of the fixed field of H. The condition on χ, namely that the set of elements g such that $\chi(g) = 0$, is satisfied provided that H is a proper subgroup of the Galois group. In this way, we can retrieve the earlier result about the vanishing of the coefficients of the Dedekind zeta function.

If χ is an irreducible character of the Galois group, then it is a classical result of Burnside (see Isaacs [Is, p. 40]) that there exist elements g such that $\chi(g) = 0$ whenever $\chi(1) > 1$. The proof of this fact is not difficult. For the sake of completeness, we sketch it here. The first step is to show that if G is a finite cyclic group, and S is the set of elements that generate G, then for any character (possibly reducible) of G, we have

$$\sum_{s \in S} |\chi(s)|^2 \geq |S|,$$

whenever $\chi(s) \neq 0$ for all $s \in S$. Indeed, the product

$$\prod_{s \in S} |\chi(s)|^2$$

is an element of the cyclotomic field $\mathbb{Q}(\zeta_n)$, where $n = |G|$ and it is invariant under the action of the Galois group of $\mathbb{Q}(\zeta_n)/\mathbb{Q}$. Since the product is non-zero, it must be ≥ 1. The result follows by applying the arithmetic-geometric mean inequality. If now, χ is an irreducible character of a group G with $\chi(1) > 1$, the second step is to partition G into equivalence classes of elements that generate the same cyclic subgroup. If $\chi(g) \neq 0$ for all $g \in G$, then for each equivalence class S, we have by the above

$$\sum_{s \in S} |\chi(s)|^2 \geq |S|.$$

Summing this over all equivalence classes of non-identity elements gives

$$\sum_{g \neq 1} |\chi(g)|^2 \geq |G| - 1.$$

But as χ is irreducible, we have

$$|G| = \sum_{g \in G} |\chi(g)|^2 \geq |G| - 1 + \chi(1)^2,$$

which is a contradiction if $\chi(1) > 1$.

4. The sieve of Eratosthenes.

The classical method of Eratosthenes allows us to deduce a crude estimate for the sum function in Theorem 1, which is useful in many instances when,

for example, the hypothesis of Theorem 1 are not satisfied. If we let $\mathcal{P}(z)$ to be the product of the primes $p \in \mathcal{P}$, with $p \leq z$, then the usual inclusion-exclusion principle gives the upper bound

$$\sum_{n \leq x} a_n = \sum_{d | \mathcal{P}(z)} \mu(d) \left[\frac{x}{d}\right] \leq x \prod_{\substack{p \in \mathcal{P} \\ p \leq z}} \left(1 - \frac{1}{p}\right) + O(2^z). \tag{1}$$

This simple inequality allows us to prove:

Theorem 2. *Suppose that*

$$\sum_{p \leq z, p \in \mathcal{P}} \frac{1}{p} \geq \alpha \log\log z + O(1).$$

Then,

$$\sum_{n \leq x} a_n \ll \frac{x}{(\log\log x)^\alpha}.$$

Proof. We apply the elementary inequality $1 - t \leq e^{-t}$ to the product in (1) to deduce

$$\sum_{n \leq x} a_n \leq x \exp\left(- \sum_{p \leq z, p \in \mathcal{P}} \frac{1}{p}\right) + O(2^z).$$

Choosing $z = c \log x$, with c sufficiently small, gives the result. ∎

As indicated in [MS],Theorem 2 can be sharpened by observing that in the sum in (1), we have the condition that $d \leq x$. If we denote by $G(x, z)$ the number of $n \leq x$ all of whose prime factors are $\leq z$ and belong to $\mathcal{P}$, then, the estimate (1) can be written as

$$\sum_{n \leq x} a_n \leq x \sum_{d | \mathcal{P}(z), d \leq x} \frac{\mu(d)}{d} + O(G(x, z)). \tag{2}$$

When $\mathcal{P}$ is the set of all prime numbers, the function $G(x, z)$ has been well studied in sieve theory and precise information about its behaviour exists. For our purposes however, we can derive an elementary estimate following Rankin (see [M, p. 130]) in our slightly general context.

Lemma 3. *Suppose that*

$$\sum_{p\le z, p\in\mathcal{P}} \frac{\log p}{p} \le \alpha \log x + O(1).$$

Then,

$$G(x,z) \ll x(\log z)^{\alpha} \exp\left(-\frac{\log x}{\log z}\right).$$

Proof. For any $\delta > 0$, we clearly have

$$G(x,z) \le \sum_{n\le x}{}' \left(\frac{x}{n}\right)^{\delta}$$

where the dash on the summation indicates that $p|n$ implies $p \le z, p \in \mathcal{P}$. Writing $\delta = 1-\eta$, and using the inequality $e^t \le 1 + te^t$, we obtain

$$G(x,z) \le x \exp\left(-\eta \log x + \sum_{p\le z, p\in\mathcal{P}} \frac{1}{p} + \eta z^{\eta} \sum_{p\le z, p\in\mathcal{P}} \frac{\log p}{p}\right).$$

By partial summation

$$\sum_{p\le z, p\in\mathcal{P}} \frac{1}{p} \le \alpha \log\log z + O(1).$$

Inserting this estimate as well as the estimate in the hypothesis, we obtain

$$G(x,z) \le x \exp\left(-\eta \log x + \alpha \log\log z + \eta z^{\eta}(\alpha \log z + O(1))\right).$$

We choose $\eta = 1/\log z$ to obtain

$$G(x,z) \ll x(\log z)^{\alpha} \exp\left(-\frac{\log x}{\log z}\right).$$

This completes the proof. ∎

Lemma 3 allows us to insert a very good estimate for the error term in (2). However, it remains to consider the main term. This is handled as in [MS]. Clearly,

$$\sum_{d|\mathcal{P}(z), d\le x} \frac{\mu(d)}{d} = \sum_{d|\mathcal{P}(z)} \frac{\mu(d)}{d} - \sum_{d|\mathcal{P}(z), d>x} \frac{\mu(d)}{d}.$$

We estimate the latter sum in the following lemma.

Lemma 4. *If*

$$\sum_{p\le z, p\in\mathcal{P}} \frac{\log p}{p} \le \alpha \log z + O(1),$$

then,

$$\sum_{d|\mathcal{P}(z), d>x} \frac{1}{d} \ll (\log z)^{\alpha+1} \exp\left(-\frac{\log x}{\log z}\right).$$

Proof. Clearly, the sum in question is by partial summation,

$$\ll \int_x^\infty \frac{G(t,z)}{t^2} dt$$

and inserting the estimate from Lemma 3, and changing variables, we are reduced to estimating

$$(\log z)^{1+\alpha} \int_{\frac{\log x}{\log z}}^\infty e^{-u} du.$$

The integral is estimated as

$$\ll \exp\left(-\frac{\log x}{\log z}\right),$$

which implies the result. ∎

We can combine both of these lemmas and deduce:

Theorem 5. *Suppose that*

$$\sum_{p\le z, p\in\mathcal{P}} \frac{\log p}{p} \le \alpha \log z + O(1).$$

Then,

$$\sum_{n\le x} a_n = x \prod_{p\le z, p\in\mathcal{P}} \left(1-\frac{1}{p}\right) + O\left(x(\log z)^{\alpha+1} \exp\left(-\frac{\log x}{\log z}\right)\right). \tag{3}$$

Corollary 6. *If in addition, we have*

$$\sum_{p\le z, p\in\mathcal{P}} \frac{\log p}{p} = \alpha \log z + O(1),$$

then

$$\sum_{n\le x} a_n \ll x \left(\frac{\log\log x}{\log x}\right)^{\alpha}.$$

Proof. By partial summation, the hypothesis implies

$$\sum_{p\le z, p\in\mathcal{P}} \frac{1}{p} = \alpha \log\log z + O(1).$$

As explained before, inserting this fact into the main term gives us an estimate of

$$\frac{x}{(\log z)^{\alpha}}$$

for the term involving the product in (3). If we choose

$$\log z = \frac{A \log x}{\log\log x}$$

for a sufficiently large constant A, we immediately obtain the result. ∎

It is possible to get a slightly better result than this with a sharper choice of z. The improvement is only marginal and any effort in that direction seems to destroy the elementary nature of the derivation. (See the remark on p. 1110 in [MS].)

References

[D] P. Deligne, Formes modulaires et représentations ℓ-adiques, *Séminaire Bourbaki, 1968 /69, exposé 355*, p. 139-172. - Berlin, Springer - Verlag, 1971 (Lecture Notes in Mathematics, 179).

[Is] M. Isaacs, Character Theory of Finite Groups, 1976, Dover.

[M] M. Ram Murty, Problems in Analytic Number Theory, GTM/RIM, Vol 206, Springer-Verlag, 2001.

[MS] M. Ram Murty and N. Saradha, On the sieve of Eratosthenes, *Canadian Journal of Mathematics,* **39** (1987), 1107-1122.

[Se] J.-P. Serre, Divisibilité de certaines fonctions arithmétiques, *L'Enseignement Math.,* **22** (1976), 227-260.

[S] J.-P. Serre, Linear representations of Finite Groups, Graduate Texts in Mathematics, Vol. 42, Springer-Verlag, 1977.

M. Ram Murty,
Department of Mathematics,
Queen's University,
Kingston, Ontario,
K7L 3N6, Canada
murty@mast.queensu.ca