ROCKY MOUNTAIN
JOURNAL OF MATHEMATICS
Volume 15, Number 2, Spring 1985

NOTES ON CHEBYSHEV'S METHOD

JOHN B. FRIEDLANDER[1]

Dedicated to the Memory of E. G. Straus and R. A. Smith

1. Introduction. The elementary method of Chebyshev for studying the distribution of primes begins with the beautiful formula

$$n! = \prod_{p \leqq n} p^{[n/p]+[n/p^2]+\cdots}.$$

For convenience, we take logarithms, getting

$$\sum_{j \leqq n} \log j = \sum_{p \leqq n} ([n/p] + [n/p^2] + \cdots) \log p.$$

Since the left hand side is easily seen to be asymptotic to $n \log n$ we deduce that there exist primes, that they are not too few (or too many), and not all small.

More generally, consider a sequence of non-negative reals, $\mathscr{A} = \{a_1, a_2, \ldots\}$, perhaps the characteristic function of an "interesting" set S of integers.

As is the case with sieve methods we attempt to derive information from the sums

$$A(X, d) = \sum_{\substack{n \leqq X \\ n \equiv 0 (d)}} a_n$$

which we write as

$$A(X, d) = A(X)/f(d) + R(X, d)$$

where $A(X) = A(X, 1)$ and where we regard $R(X, d)$ as an error term. The function f is assumed to be multiplicative. (This usually occurs in practice; in fact we shall need it only in §3). We proceed to make a number of assumptions familiar from sieve theory. (These are by and large stronger than necessary, being made with a view to §3.)

(A1) For some real $\kappa \geqq 0$ we have

$$\sum_{m \leqq X} \Lambda(m)/f(m) = \kappa \log X + O(1).$$

1. Research partially supported by an N.S.E.R.C. grant.

Received by the editors August 15, 1983.

(A2) $$\int_1^X A(t)\, dt/t = \mathrm{o}\,(A(X) \log X).$$

The Chebyshev identity is now

(1.1) $$\sum_{n \leq X} a_n \log n = \sum_{n \leq X} a_n \sum_{d \mid n} \Lambda(d) = \sum_d \Lambda(d) A(X, d).$$

Partial summation together with (A2) show that the left hand side of (1.1) is asymptotic to $A(X)\log X$. To proceed further we need an assumption that the remainders are small on average:

(A3) For some positive real $\theta < \kappa^{-1}$, and $Y = X^{\theta}$, we have

$$\sum_{d \leq Y} \Lambda(d) R(X, d) = \mathrm{o}(A(X)\log X).$$

The right hand side of (1.1) may be written as

$$A(X) \sum_{d \leq Y} \frac{\Lambda(d)}{f(d)} + \sum_{d \leq Y} \Lambda(d) R(X, d) + \sum_{d > Y} \Lambda(d) A(X, d).$$

From (A1) and (A3) we deduce

(1.2) $$\sum_{d > Y} \Lambda(d) A(X, d) \sim (1 - \kappa\theta) A(X) \log X$$

and, if we may neglect the higher prime powers by means of, say,

(A4) $$\sum_{\substack{p^k > Y \\ k \geq 2}} A(X, p^k) = \mathrm{o}(A(X))$$

we then have

(1.3) $$\sum_{Y < p \leq P} A(X, p) \log p \sim (1 - \kappa\theta) A(X) \log X.$$

Here we have denoted by P, the largest prime factor of any $n \leq X$ for which $a_n > 0$.

We deduce that there exist $a_n \neq 0$ with $n \leq X$ divisible by some $p > Y$. One would like to deduce that the set in question contains primes. This requires the sequence to have the property $a_n \neq 0$, $p \mid n \Rightarrow a_p \neq 0$, and this almost never happens. In the case $a_n = 1\ \forall n$ we have the required property and we get Chebyshev's lower bound for $\pi(X)$. In the case where we take a_n to be the number of ideals of norm n in a fixed number field, we get the property often enough to give **[4]** bounds which are not known to follow from analytic arguments.

2. The Chebyshev-Hooley method. In most sets of interest the Chebyshev method does not allow one to detect primes, only integers with large prime factors (as opposed to the integers with few prime factors detected by the sieve) and it is of interest to estimate how large. Much of the work on this aspect of the method was done by Hooley in a number of beautiful papers; see, e.g., [**9**, **10**, **11**].

The problem in general resolves itself into two components.

I. How large can we take θ and still get (A3) and thus (1.3)? Sometimes there will be a trivial value for θ (obtained for $\sum_{d<Y} \Lambda(d) | R(X, d) |$) which may be improved (again as in the case with sieve methods) by expressing $R(X, d)$ in terms of exponential sums for which a non-trivial estimate may be given or in terms of Dirichlet polynomials which may be attacked by Cauchy's theorem.

II. It may be possible by means of an upper bound sieve to obtain bounds

$$\sum_{T<p\leqq 2T} A(X, p) \leqq \sum_{T<m\leqq 2T} A(X, m) \sum_{d|m} \lambda_d$$

leading to

$$\sum_{Y<p\leqq P_0} A(X, p)\log p < cA(X)\log X$$

for some $P_0 > Y$ and some $c < 1 - \kappa\theta$. This, by comparison with (1.3), gives the lower bound $P > P_0$.

EXAMPLES.

1. $S = \{m^2 + 1 \leqq X\}$. Here one has the trivial estimate $\theta = 1/2 - \varepsilon$. Hooley in his pioneering paper [**9**] showed that one could use the sieve in conjunction with estimates for Kloosterman sums to obtain $P_0 = X^{11/20}$. This has since been improved, the best estimate at this time being $P_0 = X^{3/5}$ due to Deshouillers-Iwaniec [**2**].

2. The integers in the interval $(X - Z, X]$ where $Z = X^\alpha$, $1 > \alpha > 0$ fixed. Here $\theta = \alpha - \varepsilon$ is trivial. Ramachandra [**16**] obtained $P_0 = X^{\alpha+\delta(\alpha)}$ with the aid of van der Corput estimates and Jutila [**12**] obtained $\theta = \alpha + \delta'(\alpha)$ with an improved δ' by using Vinogradov's method. (Vaughan's identity can also be used for this.) It should be mentioned that in the case where α is small (A4) is not known to hold and this somewhat complicates the argument.

3. $S = \{p + a \mid p \leqq X\}$. In this case there is no trivial value of θ but $\theta = 1/2 - \varepsilon$ is an immediate consequence of the Bombieri-Vinogradov theorem. With the aid of this and Brun-Tichmarsh, Goldfeld [**7**] and Motohashi [**13**] independently obtained $P_0 = X^{(1/2)+\delta}$ with a δ which has been improved several times most recently by Deshouillers and Iwaniec [**3**].

There are a number of other interesting examples of results of this type, in particular a two-variable version due to Greaves [**8**] which gives estimates for large prime factors of binary forms and a conditional treatment due to Hooley [**11**] of the analogue to example 1 for cubic polynomials.

It is also possible [5, 6] to adapt the method to prove that stronger quantitative results hold when one asks only for large prime factors amongst "almost all" sequences of a given type. Finally, it should be mentioned that there are, in the case where $\mathscr{A}$ is an arithmetic progression, results of the same type. These seem not to have been investigated in the literature.

3. Other aspects of the method. From the point of view of generating functions Chebyshev's method is nothing more than the trivial identity

$$(-\zeta'(s)/\zeta(s))\zeta(s) = -\zeta'(s). \tag{3.1}$$

One can think of this as "undoing a sieve". In §2 we were concerned with finding in $\mathscr{A}$ integers with factors (large primes) which survive a sieve. One can replace that sieve by others. Thus, for example, in the case where one wishes to find large squarefree factors, one has the equally trivial identity

$$(\zeta(s)/\zeta(2s))\zeta(2s) = \zeta(s). \tag{3.2}$$

We restrict our consideration here to the integers in the interval $(X - Z, X]$ as in example 2. We have

$$\sum_{X-Z<n\leq X} = \sum_{r\leq X} \mu^2(r)\left(\left[\left(\frac{X}{r}\right)^{1/2}\right] - \left[\left(\frac{X-Z}{r}\right)^{1/2}\right]\right)$$
$$= \sum_{r>Y} + \sum_{r\leq Y},$$

say where Y is chosen (as large as possible) so that

$$\sum_{r\leq Y} \mu^2(r)\left(\left\{\left(\frac{X}{r}\right)^{1/2}\right\} - \left\{\left(\frac{X-Z}{r}\right)^{1/2}\right\}\right) = o(Z). \tag{3.3}$$

since

$$(X^{1/2} - (X-Z)^{1/2}) \sum_{r\leq Y} \frac{\mu^2(r)}{(r^{1/2})} \ll X^{1/2}ZX^{-1}Y^{1/2} = o(Z),$$

provided $Y = o(X)$, we deduce that

$$Z \sim \sum_{r>Y} \mu^2(r)\left(\left[\left(\frac{X}{r}\right)^{1/2}\right] - \left[\left(\frac{X-Z}{r}\right)^{1/2}\right]\right)$$

and that the interval contains an integer with a squarefree factor $> Y$.

The trivial estimate for (3.3) allows only the same estimate as for the largest prime factor but the relevant exponential sums

$$\sum_{r\leq R} \mu^2(r)e\left(\left(\frac{X}{r}\right)^{1/2}\right)$$

can be estimated somewhat more efficiently than the corresponding sums [12] for primes.

If instead of square-free factors, one is interested in factors which are almost-primes, as for instance when the sequence $\mathscr{A}$ has a larger value of κ (e.g., reducible polynomials) then an appropriate identity is given by

$$((-1)^r \zeta^{(r)}(s)/\zeta(s))\zeta(s) = (-1)^r\zeta^{(r)}(s). \tag{3.4}$$

Here

$$(-1)^r\zeta^{(r)}(s)/\zeta(s) = \sum_{n\geqq 1} \frac{\Lambda_r(n)}{n^s}$$

where the generalized von Mangoldt functions Λ_r, see, e.g., **[1]**, have the properties:

$$\Lambda_r(n) \geqq 0,$$
$$\Lambda_r(n) > 0 \Leftrightarrow 1 \leqq \nu(n) \leqq r, \text{ and}$$
$$\sum_{d\mid n} \Lambda_r(d) = \log^r n.$$

Arguing as in §1,

$$\sum_{n\leqq X} a_n \log^r n = \sum_d \Lambda_r(d)A(X, d)$$
$$= A(X)\sum_{d\leqq Y} \frac{\Lambda_r(d)}{f(d)} + \sum_{d\leqq Y} \Lambda_r(d)R(X, d) + \sum_{d>Y} \Lambda_r(d)A(X, d)$$

and, replacing (A3) by the assumption

$$\sum_{d\leqq Y} \Lambda_r(d)R(X, d) = o(A(X)\log^r X), \tag{A5}$$

we deduce that

$$\sum_{d>Y} \Lambda_r(d)A(X, d) \sim c(\kappa, r, \theta)A(X)\log^r X, \tag{3.5}$$

where

$$c(\kappa, r, \theta) = 1 - \theta^r \frac{\kappa(\kappa + 1) \cdots (\kappa + r - 1)}{r!}.$$

This may be proved by induction on r with the aid of the identity

$$\Lambda_{r+1}(n) = \Lambda_r(n)\log n + \sum_{d\mid n} \Lambda_r(d)\Lambda(n/d)$$

which also follows by induction on r.

4. Integers without large prime factors. In this section we discuss briefly the problem complementary to that in §2. For definiteness we again confine ourselves to the case of example 2, the integers in the interval $(X - Z, X]$. The results of this section represent work done jointly with J.C. Lagarias.

Consider $(X - Z, X]$, $Z = X^{\alpha}$, $Y = X^{\theta}$ where $0 < \alpha < 1$ and $0 < \theta < 1$ are fixed. Arguing as in §1,

$$\sum_{p>Y} A(X, p)\log p < (1 - \theta + o(1))Z \log X. \tag{4.1}$$

(Recall that we do not have (A4) but, for this problem, the inequality goes the right way and we can neglect higher powers of primes.)

Suppose now that each $n \in S$ is divisible by some prime $> X^{\beta} > Y$. The left side of (4.1) thus exceeds $\beta Z \log X$ and so $\beta \leqq 1 - \theta$.

DEFINITION 4.2. $f(\alpha)$ is the inf of those F such that, as $X \to \infty$, the interval $(X - X^{\alpha}, X]$ contains a positive proportion of integers all of whose prime factors are $\leqq X^{F}$.

By the above argument combined with the estimate of Jutila **[12]** referred to in §2, we have:

THEOREM 4.3. *For* $0 < \alpha < 1/2$, *there exists* $\delta(\alpha) > 0$ *such that* $f(\alpha) < 1 - \alpha - \delta$.

We remark that Turk **[17]** has independently proved essentially the same result, and that Pomerance **[14]**, who seems to have been the first to consider the complementary problem, has investigated example 3 (shifted primes). See also **[5, 6]**.

Since $f(\alpha)$ is obviously non-increasing, one gets from the above, trivial results for $\alpha \geqq 1/2$. To do better, for instance, to show $f(\alpha) \to 0$ as $\alpha \to 1^{-}$, one needs to have an inclusion-exclusion argument which requires in turn some control on the contribution from multiples of almost-primes. The formula (3.5) is adequate for this purpose and with its aid one can prove the following result.

THEOREM 4.4. *As* $\alpha \to 1^{-}$, $f(\alpha) \to 0$ *and, in fact,*

$$f(\alpha) \ll \frac{\log\log(1/(1 - \alpha))}{\log(1/(1 - \alpha))}.$$

Or course it is very probably true that $f(\alpha)$ is identically zero. It would be nice even to have the result that $f(\alpha) = 0$ for some $\alpha < 1$.

A result like (4.4) holds (conditionally), see Pomerance **[15]**, for the case of $\{p + a\}$ if it is assumed that (A3) holds with $\theta = \alpha$.

REFERENCES

1. E. Bombieri, *The asymptotic sieve*, Rend. Accad. Naz. **XL**, Ser. 5, 1/2 (1975–77) 243–269.

2. J. M. Deshouillers and H. Iwaniec, *On the greatest prime factor of* $n^2 + 1$, Ann. Inst. Fourier, Gernoble 32, 4 (1982) 1–11.

3. _____, *On the Brun-Titchmarsh theorem and the greatest prime factor of* $p + a$, Colloq. Math. Janos Bolyai Vol. 34, to appear.

4. J. B. Friedlander, *Estimates for prime ideals*, J. Number Theory **12** (1980) 101–105.

5. ———, *Large prime factors in small intervals*, Colloq. Math. Janos Bolyai, Vol. 34, to appear.

6. ———, *Integers without large prime factors* III, Arch. Math. **43** (1984) 32–36.

7. M. Goldfeld, *On the number of primes p for which p + a has a large prime factor*, Mathematika **16** (1969), 23–27.

8. G. Greaves, Large prime factors of binary forms, J. Number Theory **3** (1971) 35–59; Correction ibid. **9** (1977) 561–562.

9. C. Hooley, *On the greatest prime factor of a quadratic polynomial*, Acta Math. **117** (1967) 281–299.

10. ———, *Applications of Sieve Methods to the Theory of Numbers*, Cambridge Tracts in Mathematics **70**, Cambridge 1976.

11. ———, *On the greatest prime factor of a cubic polynomial*, J. Reine Angew. **303/304** (1978) 21–50.

12. M. Jutila, *On numbers with a large prime factor* II, J. Indian Math. Soc. **38** (1974) 125–130.

13. Y. Motohashi, *A note on the least prime in an arithmetic progression with a prime difference*, Acta Arith. **17** (1970) 283–285.

14. C. Pomerance, *Popular values of Euler's function*, Mathematika **27** (1980) 84–89.

15. ———, *A new lower bound for the pseudoprime counting function*, Illinois J. Math. **26** (1982) 4–9.

16. K. Ramachandra, *A note on numbers with a large prime factor* II, J. Indian Math. Soc. **34** (1970) 39–48.

17. J. W. M. Turk, *Products of integers in short intervals*, Report 8228M, Econometric Inst., Erasmus Univ., Rotterdam. 1982.

SCARBOROUGH COLLEGE UNIVERSITY OF TORONTO
INSTITUTE FOR ADVANCED STUDY PRINCETON, NJ 08540

ADDED IN PROOF. Since, this paper was written J.C. Lagarias and the author (to appear) have greatly improved the results of §4. They prove that, for $0 < \alpha < 1$, and some c,

$$f(\alpha) < 1 - \alpha - c\alpha^3(1 - \alpha),$$

and that stronger results follow (by different methods) if one does not require a positive proportion of integers in the definition of f.

Independently, results on this topic have now been given also by A. Hildebrand and G. Tenenbaum and by A. Balog and A. Sarközy.

The topic of §2, in the case of arithmetic progressions, has now been studied by the author jointly with A. Balog and J. Pintz. (Studia Sci. Math. Hungar., to appear.)