Conspectus materiae tomi XXIV, fasciculi 2

La revue est consacrée à la Théorie des Nombres
The journal publishes papers on the Theory of Numbers
Die Zeitschrift veröffentlicht Arbeiten aus der Zahlentheorie
Журнал посвящен теории чисел

L'adresse de la Rédaction et de l'échange
Address of the Editorial Board and of the exchange
Die Adresse der Schriftleitung und des Austausches
Адрес редакции и книгообмена

ACTA ARITHMETICA
ul. Śniadeckich 8, 00-950 Warszawa

Les auteurs sont priés d'envoyer leurs manuscrits en deux exemplaires
The authors are requested to submit papers in two copies
Die Autoren sind gebeten um Zusendung von 2 Exemplaren jeder Arbeit
Рукописи статей редакция просит предлагать в двух экземплярах

PRINTED IN POLAND

WROCŁAWSKA DRUKARNIA NAUKOWA

ACTA ARITHMETICA
XXIV (1973)

Brun's method and the Fundamental Lemma

by

H. Halberstam (Nottingham) and H.-E. Richert (Ulm)

Dedicated to C. L. Siegel

1. Introduction. Let $\mathscr{A}$ be a finite sequence of (not necessarily distinct nor necessarily positive) integers, and let $\mathscr{P}$ be a set of primes. Let $\overline{\mathscr{P}}$ denote the complement of $\mathscr{P}$ with respect to the set $\mathscr{P}_1$ of all primes, and let $(d, \overline{\mathscr{P}}) = 1$ signify that d has no prime factors in $\overline{\mathscr{P}}$. For any real number $z \geqslant 2$ we shall write

$$P(z) := \prod_{\substack{p<z \\ p\in\mathscr{P}}} p.$$

To 'sift' $\mathscr{A}$ by the primes of $\mathscr{P}$ less than z is to eliminate from $\mathscr{A}$ all those elements a of $\mathscr{A}$ that are divisible by a prime $p < z, p \in \mathscr{P}$, and many arithmetical questions depend on being able to count the number of elements of $\mathscr{A}$ that survive this 'sieve' process. Accordingly, we shall concern ourselves with the 'sifting' function

$$S(\mathscr{A}; \mathscr{P}, z) := \big|\{a\colon\ a \in \mathscr{A}, (a, P(z)) = 1\}\big|,$$

where $|\{\ldots\}|$ denotes the cardinality of the set $\{\ldots\}$. There are no (significant) estimates of $S(\mathscr{A}; \mathscr{P}, z)$ that are valid for all sequences $\mathscr{A}$ and all sifting sets $\mathscr{P}$, and we shall now introduce some basic restrictions on the nature of $\mathscr{A}$ and $\mathscr{P}$. To this end we postulate the existence of a real number $X > 1$ and a non-negative multiplicative arithmetic function $\omega(d)$ on the sequence of squarefree integers d such that

$$\omega(p) = 0 \quad \text{if} \quad p \in \overline{\mathscr{P}},$$

and

$$(\Omega_1) \qquad \frac{\omega(p)}{p} \leqslant 1 - \frac{1}{A_1}$$

for some constant $A_1 \geqslant 1$;

$$(\Omega_2(\varkappa)) \qquad \sum_{w \leqslant p < z} \frac{\omega(p)}{p} \log p \leqslant \varkappa \log\frac{z}{w} + A_2, \quad 2 \leqslant w \leqslant z,$$

for some pair of constants $\varkappa > 0$ and $A_2 \geqslant 1$; and such that the remainders R_d given by

$$R_d := \sum_{\substack{a\in\mathscr{A}\\ a\equiv 0 \bmod d}} 1 - \frac{\omega(d)}{d}X$$

satisfy

$$\text{(R)} \qquad |R_d| \leqslant K\omega(d) \quad \text{if} \quad \mu(d) \neq 0,\ (d, \overline{\mathscr{P}}) = 1$$

for some real number $K \geqslant 1$ [1]. Thus the remainders R_d with d squarefree and satisfying $(d, \overline{\mathscr{P}}) = 1$ are, in a certain sense, small; in particular,

$$|R_1| = \big||\mathscr{A}| - X\big| \leqslant K,$$

so that X is some convenient approximation to the cardinality of $\mathscr{A}$. All our main results should be viewed against the background of the parameter X (and also of z) tending to infinity.

Let

$$V(z) := \prod_{p<z}\left(1 - \frac{\omega(p)}{p}\right).$$

On probabilistic grounds one expects $S(\mathscr{A}; \mathscr{P}, z)$ to be roughly equal to $XV(z)$; but, taking $\mathscr{A}$ to be the set $\{n: 1 \leqslant n \leqslant X\}$, $\mathscr{P} = \mathscr{P}_1$ and $z = X^{\frac{1}{2}}$, one can check easily that this cannot be true in general. On the other hand, such a result is certainly valid, indeed quite generally, if z is constant, or very small compared with X (see Theorem 1 below); and there is therefore the natural problem of determining the most extensive region in the X-z plane within which

$$\text{(1.1)} \qquad S(\mathscr{A}; \mathscr{P}, z) \sim XV(z) \quad \text{as} \quad X \to \infty,\ z \to \infty.$$

A *Fundamental Lemma*, in the context of sieve theory, is any result which establishes (1.1) for some region of the X-z plane. The quality of a Fundamental Lemma depends chiefly on two factors: (i) the extensiveness of the associated region, and (ii) on the precision with which the remainder

$$\left|\frac{S(\mathscr{A}; \mathscr{P}, z)}{XV(z)} - 1\right|$$

can be estimated.

Our object in this paper is to prove a Fundamental Lemma of high quality (see Theorem 4 below), and to give some applications. Our main tool is Brun's sieve method. We present in Section 3 a new and simple account of this method (cf. Levin [7]), and we use it to establish a general sieve result in Theorem 3 below. A somewhat weaker version of Theorem 3 appeared recently in our note [1], where we also indicated briefly how to derive from it a good Fundamental Lemma. Unfortunately, [1] was full of misprints and minor errors [2], and we shall therefore make no reference here to any of the calculations or arguments contained in [1]. A noteworthy feature of Theorem 4 is that a result of this quality cannot be obtained by Selberg's method, at any rate not without the use of some additional new idea.

[1] All O-constants and $B, B_1, \ldots, B_4$ depend at most on A_1, A_2 and $\varkappa$; they do not depend on K (or on X and z).

2. Two simple Fundamental Lemmas.

2. Two simple Fundamental Lemmas. We begin with an auxiliary result.

LEMMA 1 $(\Omega_2(\varkappa))$ [3]. *If $2 \leqslant w \leqslant z$, then*

$$\text{(2.1)} \qquad \sum_{w \leqslant p < z} \frac{\omega(p)}{p} \leqslant \varkappa \log\frac{\log z}{\log w} + \frac{A_2}{\log w},$$

$$\text{(2.2)} \qquad \sum_{p<z} \omega(p) \leqslant (\varkappa + A_2)\,\mathrm{li}\,z + \frac{2A_2}{\log 2} \leqslant A(2\,\mathrm{li}\,z + 3), \qquad A := \max(\varkappa, A_2),$$

and, if also (Ω_1) *is satisfied, then*

$$\text{(2.3)} \qquad \sum_{p<z} g(p) \leqslant \varkappa\log\log z + \varkappa\log\frac{1}{\log 2} + \frac{A_2}{\log 2}\left\{1 + A_1\left(\varkappa + \frac{A_2}{\log 2}\right)\right\},$$

where

$$g(p) := \frac{\omega(p)}{p - \omega(p)},$$

$$\text{(2.4)} \qquad \frac{V(w)}{V(z)} \leqslant \left(\frac{\log z}{\log w}\right)^{\varkappa} \exp\left(\frac{2B}{\log w}\right), \qquad B := \frac{A_2}{2}\left\{1 + A_1\left(\varkappa + \frac{A_2}{\log 2}\right)\right\},$$

and, in particular,

$$\text{(2.5)} \qquad \frac{1}{V(z)} = O(\log^{\varkappa} z).$$

Proof. Here (2.1) and (2.3) are the right hand inequalities in (2.4) and (2.5) (with $w = 2$) of [2], respectively; (2.4) follows from (2.9) and (2.5) of [2], and (2.5) follows from (2.4) on putting $w = 2$. It is important

[2] Notwithstanding these errors, all the main results of [1] are true; this refers in particular to all the applications of Brun's Sieve in [1]. Apart from the Fundamental Lemma itself, we shall therefore not deal with these applications again here.

[3] 'Lemma 1 $(\Omega_2(\varkappa))$: ...' signifies that the conclusions of Lemma 1 have been proved under the condition $(\Omega_2(\varkappa))$. We shall use this notation throughout the paper.

to note that all the upper inequalities cited from [2] depend only on $\big(\Omega_2(\varkappa)\big)$. It remains to prove (2.2). We have, using (2.1),

$$\sum_{p<z}\omega(p) = 2\sum_{p<z}\frac{\omega(p)}{p}+\int_2^z\sum_{w\leqslant p<z}\frac{\omega(p)}{p}\,dw$$
$$\leqslant 2\varkappa\log\frac{\log z}{\log 2}+\frac{2A_2}{\log 2}+\int_2^z\left(\varkappa\log\frac{\log z}{\log w}+\frac{A_2}{\log w}\right)dw$$
$$=\frac{2A_2}{\log 2}+(\varkappa+A_2)\operatorname{li}z,$$

whence the result.

We have obviously that

$$S(\mathscr{A};\mathscr{P},z) = \sum_{a\in\mathscr{A}}\sum_{\substack{d|a\\ d|P(z)}}\mu(d) = \sum_{d|P(z)}\mu(d)\sum_{\substack{a\in\mathscr{A}\\ a\equiv 0 \bmod d}}1 \tag{2.6}$$
$$= X\sum_{d|P(z)}\frac{\mu(d)\,\omega(d)}{d}+\sum_{d|P(z)}\mu(d)R_d$$
$$= XV(z)+\theta\sum_{d|P(z)}|R_d|,\qquad |\theta|\leqslant 1;$$

and we deduce at once that

Theorem 1 $\big(\Omega_2(\varkappa)\big)$, (R). *We have*

$$S(\mathscr{A};\mathscr{P},z) = XV(z)+\theta Ke^{A(2\operatorname{li}z+3)},\qquad |\theta|\leqslant 1.$$

We may regard Theorem 1 as resting on the original sieve idea of Eratosthenes, as formalized by Legendre (also by Meissel and others). Theorem 1 yields a Fundamental Lemma of rather poor quality. For if we assume also that (Ω_1) is satisfied, then $1/V(z)$ is of order of magnitude $\log^{\varkappa}z$ (cf. (2.5)) and therefore, even if K is bounded, Theorem 1 implies (1.1) only when z is not much larger than $\log X$ (to be precise, z would have to be less than some small constant multiple of $\log X\log\log X$).

The weakness of Theorem 1 derives from the fact that the summation in the remainder term on the right of (2.6) has too many terms. We shall obtain a significant improvement (Theorem 2 below) of Theorem 1 by using the following simple idea with which Viggo Brun began his famous work on sieve methods.

Lemma 2. *For any natural number n and for any non-negative integer s, we have*

$$\sum_{\substack{d|n\\ \nu(d)\leqslant 2s+1}}\mu(d)\leqslant\sum_{d|n}\mu(d)\leqslant\sum_{\substack{d|n\\ \nu(d)\leqslant 2s}}\mu(d),$$

where $\nu(d)$ denotes the number of distinct prime factors of d.

Proof. If $n=1$ the three sums are obviously equal, so that we may suppose that $n>1$, when the middle sum is zero. Writing $\nu(n)=v$ $(\geqslant 1)$, we have

$$\sum_{\substack{d|n\\ \nu(d)=m}}\mu(d) = (-1)^m\binom{v}{m},$$

a statement that is consistent with the convention $\binom{v}{m}=0$ for $v<m$. Hence, for any non-negative integer k,

$$\sigma^{(k+1)}(n):=\sum_{\substack{d|n\\ \nu(d)\leqslant k}}\mu(d) = \sum_{m=0}^{k}(-1)^m\binom{v}{m}.$$

Since obviously

$$\sigma^{(k+2)}(n) = (-1)^{k+1}\binom{v}{k+1}+\sigma^{(k+1)}(n)$$

and

$$\binom{v}{k-1}-\binom{v-1}{k}=\binom{v-1}{k+1},$$

it follows by induction on k that

$$\sigma^{(k+1)}(n) = (-1)^k\binom{v-1}{k}, \tag{2.7}$$

and this is more than is required to prove the Lemma.

Corollary [4]. *If n and r are positive integers,*

$$\sum_{d|n}\mu(d) = \sum_{\substack{d|n\\ \nu(d)\leqslant r-1}}\mu(d)+\vartheta\sum_{\substack{d|n\\ \nu(d)=r}}\mu(d),\qquad 0\leqslant\vartheta\leqslant 1. \tag{2.8}$$

Proof. For $n=1$, (2.8) is obviously true; for $n>1$, (2.8) can be written

$$0 = \sigma^{(r)}(n)+\vartheta\big(\sigma^{(r+1)}(n)-\sigma^{(r)}(n)\big),$$

which is obviously true for a suitable ϑ by (2.7).

Using Lemma 2, we shall obtain

Theorem 2 (Ω_1), $\big(\Omega_2(\varkappa)\big)$, (R). *We have, as $X\to\infty$,*

$$S(\mathscr{A};\mathscr{P},z) = XV(z)\{1+O(e^{-\sqrt{\log X}})\}+O(KX^{1/2}),\qquad \log z\leqslant\sqrt{\log X}.$$

The rest of Section 2 is devoted to the proof of Theorem 2. We write

$$\sigma^{(r)}(n) = \sum_{d|n}\mu(d)\chi^{(r)}(d), \tag{2.9}$$

where

$$\chi^{(r)}(d) = \begin{cases}1, & \nu(d)\leqslant r-1,\\ 0 & \text{otherwise};\end{cases} \tag{2.10}$$

[4] The Corollary is given for completeness. Although it is sometimes useful (see f. e. [3]), we shall not make direct application of it here.

then, by Möbius inversion

$$\mu(d)\chi^{(r)}(d) = \sum_{\delta|d}\mu\left(\frac{d}{\delta}\right)\sigma^{(r)}(\delta). \tag{2.11}$$

By Lemma 2 we have, for any non-negative integers s, s', that

$$\sum_{a\in\mathscr{A}}\sum_{\substack{d|a\\ d|P(z)}}\mu(d)\chi^{(2s+2)}(d)\leqslant S(\mathscr{A};\mathscr{P},z)\leqslant\sum_{a\in\mathscr{A}}\sum_{\substack{d|a\\ d|P(z)}}\mu(d)\chi^{(2s'+1)}(d),$$

so that

$$X\sum_{d|P(z)}\mu(d)\chi^{(2s+2)}(d)\frac{\omega(d)}{d}-\sum_{d|P(z)}\chi^{(2s+2)}(d)|R_d|\leqslant S(\mathscr{A};\mathscr{P},z) \tag{2.12}$$

$$\leqslant X\sum_{d|P(z)}\mu(d)\chi^{(2s'+1)}(d)\frac{\omega(d)}{d}+\sum_{d|P(z)}\chi^{(2s'+1)}(d)|R_d|.$$

Letting r be any positive integer, we have, by (R) and (2.2), that

$$\sum_{d|P(z)}\chi^{(r)}(d)|R_d|\leqslant K\sum_{\substack{d|P(z)\\ \nu(d)\leqslant r-1}}\omega(d)\leqslant K\Big(1+\sum_{p<z}\omega(p)\Big)^{r-1}\leqslant Kz^{r-1} \tag{2.13}$$

provided that we assume, as we shall do from now on, that

$$z\geqslant B_1, \tag{2.14}$$

where $B_1 = B_1(\varkappa, A_2)$ is a sufficiently large constant; the assumption is justified since Theorem 2 would follow easily from Theorem 1 if z were bounded.

Inequality (2.13) disposes of the remainder terms on either side of (2.12), subject to a suitable choice of s and s'. It remains to deal with the leading terms. We have, by (2.11), that

$$\sum_{d|P(z)}\mu(d)\chi^{(r)}(d)\frac{\omega(d)}{d} = \sum_{d|P(z)}\frac{\omega(d)}{d}\sum_{\delta|d}\mu\left(\frac{d}{\delta}\right)\sigma^{(r)}(\delta) \tag{2.15}$$

$$= \sum_{\delta|P(z)}\sigma^{(r)}(\delta)\frac{\omega(\delta)}{\delta}\sum_{t\left|\frac{P(z)}{\delta}\right.}\mu(t)\frac{\omega(t)}{t}$$

$$= \sum_{\delta|P(z)}\sigma^{(r)}(\delta)\frac{\omega(\delta)}{\delta}\prod_{t\left|\frac{P(z)}{\delta}\right.}\left(1-\frac{\omega(p)}{p}\right)$$

$$= V(z)\sum_{\delta|P(z)}\sigma^{(r)}(\delta)g(\delta)$$

$$= V(z)\Big\{1+\sum_{1<\delta|P(z)}\sigma^{(r)}(\delta)g(\delta)\Big\},$$

where

$$g(\delta) = \prod_{p|\delta}\frac{\omega(p)}{p-\omega(p)},\qquad \mu(\delta)\neq 0,$$

so that $g(\delta)$ is a non-negative, multiplicative function on the sequence of squarefree numbers, which is well defined by virtue of (Ω_1).

Next, by (2.7),

$$|\sigma^{(r)}(n)| = \left|\binom{\nu(n)-1}{r-1}\right|\leqslant\binom{\nu(n)}{r}\quad\text{if}\quad n>1,$$

so that

$$\sum_{1<\delta|P(z)}\sigma^{(r)}(\delta)g(\delta)\leqslant\sum_{1<\delta|P(z)}\binom{\nu(\delta)}{r}g(\delta)$$

$$=\sum_{m=r}^{\nu(P(z))}\binom{m}{r}\sum_{\substack{1<\delta|P(z)\\ \nu(\delta)=m}}g(\delta)\leqslant\sum_{m=r}^{\infty}\binom{m}{r}\frac{1}{m!}\Big(\sum_{p<z}g(p)\Big)^m$$

$$=\frac{1}{r!}\Big(\sum_{p<z}g(p)\Big)^r\exp\Big(\sum_{p<z}g(p)\Big).$$

Hence, by (2.12), (2.13) and (2.15), we have for any positive integer r, that

$$S(\mathscr{A};\mathscr{P},z) = XV(z)\Big\{1+\theta\frac{1}{r!}\Big(\sum_{p<z}g(p)\Big)^r\exp\Big(\sum_{p<z}g(p)\Big)\Big\}+\theta' Kz^{r-1}, \tag{2.16}$$

$$|\theta|\leqslant 1,\ |\theta'|\leqslant 1.$$

By (2.3) we have

$$\sum_{p<z}g(p)\leqslant\varkappa\log\log z+B_2$$

where

$$B_2 = \varkappa\log\frac{1}{\log 2}+\frac{A_2}{\log 2}\Big\{1+A_1\Big(\varkappa+\frac{A_2}{\log 2}\Big)\Big\}.$$

We now choose r to be given by

$$r = \Big[\frac{1}{\lambda}(\varkappa\log\log z+B_2)\Big]+1$$

where λ is a parameter satisfying

$$0<\lambda e^{1+\lambda}\leqslant 1. \tag{2.17}$$

Hence

$$\sum_{p<z}g(p)\leqslant\lambda r.$$

Using the well-known estimate

$$\frac{1}{r!} \leqslant \left(\frac{e}{r}\right)^r$$

which holds for any natural number r, we obtain

$$\frac{1}{r!}\Big(\sum_{p<z} g(p)\Big)^r \exp\Big(\sum_{p<z} g(p)\Big) \leqslant \left(\frac{e}{r}\right)^r (\lambda r)^r e^{\lambda r} = (\lambda e^{1+\lambda})^r;$$

substituting in (2.16) we arrive at

$$S(\mathscr{A};\mathscr{P},z) = XV(z)\{1+\theta(\lambda e^{1+\lambda})^{\frac{1}{\lambda}(\varkappa\log\log z+B_2)}\}+\theta' Kz^{\frac{1}{\lambda}(\varkappa\log\log z+B_2)},$$
$$|\theta| \leqslant 1,\ |\theta'| \leqslant 1.$$

Finally, we choose

$$\frac{1}{\lambda} = \frac{1}{2}\,\frac{\log X}{\log z(\varkappa\log\log z+B_2)};$$

then (2.17) is satisfied provided that $\log z \leqslant \sqrt{\log X}$ and X is large enough. Indeed, in these circumstances we have even that $\lambda e^{1+\lambda} \leqslant e^{-2}$, and since

$$\frac{1}{\lambda}(\varkappa\log\log z+B_2) = \frac{1}{2}\,\frac{\log X}{\log z} \geqslant \frac{1}{2}\sqrt{\log X},$$

we have, as $X\to\infty$, that

$$S(\mathscr{A};\mathscr{P},z) = XV(z)\{1+\theta e^{-\sqrt{\log X}}\}+\theta' KX^{1/2}, \qquad |\theta| \leqslant 1,\ |\theta'| \leqslant 1,$$

which completes the proof of Theorem 2.

3. Brun's sieve. We saw in the proof of Theorem 2 that the parameter r has to be taken rather large in order to obtain an effective result, but that this compels us (cf. (2.13)) to take z smaller than we might wish. So far as the error term is concerned, we can see how to overcome this difficulty. Let us decide that the prime divisors of d in (2.9) should, apart from being at most $r-1$ in number (cf. (2.10)), also be restricted in size to the extent that at most D_1, say, of them can come from an interval $z_1 \leqslant p < z$. We should then have at once the superior estimate

$$\sum_{d|P(z)} |R_d| \leqslant \Big(1+\sum_{p<z}\omega(p)\Big)^{D_1}\Big(1+\sum_{p<z_1}\omega(p)\Big)^{r-1-D_1};$$

and if this did not suffice we could introduce a further parameter z_2, $z_2 < z_1$, and require not more than D_2 prime divisors of d to come from the interval $z_2 \leqslant p < z_1$; and so forth. Of course, such additional constraints on the numbers d introduce new difficulties so far as the determination of the leading terms are concerned; Brun showed us how to overcome these, but the expositions of Brun's method in the literature have seemed to most students of the subject to be exceedingly involved. However, a recent suggestion in Levin [7] has enabled us to formalize Brun's technique in a very simple way so that his method can be seen, almost for the first time, to be both exceptionally elegant and unexpectedly powerful.

Let χ_1 and χ_2 be arithmetical functions, taking the values 0 and 1 only, on the set of positive divisors of $P(z)$, such that for $\nu = 1$ and 2

$$\chi_\nu(1) = 1, \tag{3.1}$$

$$\chi_\nu(d) = 1 \quad \text{implies} \quad \chi_\nu(t) = 1 \quad \text{for all } t|d, \tag{3.2}$$

$$\chi_\nu(t) = 1,\ \mu(t) = (-1)^\nu \quad \text{imply} \quad \chi_\nu(pt) = 1 \quad \text{for all } p < q(t),\ p|P(z), \tag{3.3}$$

where if $n > 1$, $q(n)$ is the least prime factor of n, and $q(1) = \infty$. Taking $t = 1$ in (3.3) (and therefore $\nu = 2$) shows that (3.3) incorporates the special condition

$$\chi_2(p) = 1 \quad \text{for all } p|P(z).$$

It is clear that we may think of χ_1 and χ_2 as characteristic functions of two sets D_1 and D_2 of divisors of $P(z)$, but it turns out to be more efficient to work directly with χ_1 and χ_2 rather than through the structures of D_1 and D_2. It is easy to verify that $\chi^{(2s+1)}$ and $\chi^{(2s)}$ for any non-negative integer s are realizations of χ_1 and χ_2 respectively.

Next, we define (cf. (2.9)), for each $n|P(z)$,

$$\sigma_\nu(n) := \sum_{d|n}\mu(d)\chi_\nu(d), \qquad \nu = 1, 2;$$

and we introduce for convenience also the further notations p^+ for the successor of p in $\mathscr{P}$ (in the sense of increasing magnitude), and

$$P_{u,v} := \prod_{\substack{u\leqslant p<v\\ p\in\mathscr{P}}} p = P(v)/P(u).$$

We now make several almost obvious remarks.

Lemma 3. *If $p\in\mathscr{P}$ and $t|P_{p^+,z}$ then*

$$\chi_\nu(t)-\chi_\nu(pt) = (-1)^{\nu-1}\mu(t)\chi_\nu(t)\{1-\chi_\nu(pt)\}, \qquad \nu = 1, 2; \tag{3.4}$$

and if $d|P(z)$, then

$$\chi_\nu(d) = 1-\sum_{p|d}\{\chi_\nu((d, P_{p^+,z}))-\chi_\nu((d, P_{p,z}))\}. \tag{3.5}$$

Proof. Both sides of (3.4) vanish if $\chi_\nu(pt) = \chi_\nu(t)$, and by (3.2) this is always the case if $\chi_\nu(pt) = 1$. Hence we may suppose that $\chi_\nu(pt) = 0$,

$\chi_\nu(t) = 1$. Then, by (3.3), $\mu(t) = (-1)^{\nu-1}$ and so both sides of (3.4) are equal to 1. This proves (3.4).

Relation (3.5) is trivial if $d = 1$. If $d > 1$, say $d = p_1 \dots p_r$ with $p_1 < \dots < p_r$, $p_i \in \mathscr{P}$, the sum on the right of (3.5) equals

$$\sum_{i=1}^{r-1} \{\chi_\nu(p_{i+1} \dots p_r) - \chi_\nu(p_i \dots p_r)\} + 1 - \chi_\nu(p_r) = 1 - \chi_\nu(d).$$

LEMMA 4. *We have* $\sigma_1(1) = 1 = \sigma_2(1)$, *and*

$$\sigma_2(n) \leqslant \sum_{d|n} \mu(d) \leqslant \sigma_1(n) \quad \textit{for all } n | P(z).$$

Proof. For $n = 1$ the result is obvious from (3.1). Suppose then that $n > 1$. Here we have to show that

$$(3.6) \qquad (-1)^\nu \sigma_\nu(n) \leqslant 0 \quad \text{if} \quad n > 1,\ n | P(z);\ \nu = 1, 2.$$

But then if $q(n) = p$ and $n = pm$, so that $t | P_{p^+, z}$ for every $t | m$, we have

$$\sigma_\nu(n) = \sum_{t|m} \{\mu(t)\chi_\nu(t) + \mu(pt)\chi_\nu(pt)\} = \sum_{t|m} \mu(t)\{\chi_\nu(t) - \chi_\nu(pt)\}$$
$$= (-1)^{\nu-1} \sum_{t|m} \chi_\nu(t)\{1 - \chi_\nu(pt)\}$$

by (3.4); and (3.6) now follows immediately.

Lemma 4 is obviously a generalization of Lemma 2 to all function pairs χ_1, χ_2 satisfying the basic conditions (3.1), (3.2) and (3.3). Just as we derived (2.12) from Lemma 2, we now deduce easily from Lemma 4 that

$$(3.7) \quad (\mathrm{R}): \quad (-1)^\nu S(\mathscr{A}; \mathscr{P}, z) \geqslant (-1)^\nu X U_\nu(z) - K \sum_{d|P(z)} \chi_\nu(d)\,\omega(d), \qquad \nu = 1, 2,$$

where

$$(3.8) \qquad U_\nu(z) := \sum_{d|P(z)} \mu(d)\chi_\nu(d) \frac{\omega(d)}{d}.$$

We shall now derive for $U_\nu(z)$ a result that is in some respects analogous to (2.15); but first we introduce, as was foreshadowed at the beginning of Section 3, a partition

$$(3.9) \qquad 2 = z_r < z_{r-1} < \dots < z_1 < z_0 = z$$

of the interval $[2, z]$.

LEMMA 5 (Ω_1). *If*

$$V(w, z) := \prod_{\substack{w \leqslant p < z \\ p \in \mathscr{P}}} \left(1 - \frac{\omega(p)}{p}\right) = V(z)/V(w) \quad \textit{for } 2 \leqslant w \leqslant z,$$

then

$$U_\nu(z) = V(z)\left\{1 + \theta \sum_{n=1}^{r} \frac{1}{V(z_n, z)} \sum_{z_n \leqslant p < z_{n-1}} \frac{\omega(p)}{p} \sum_{t|P_{p^+, z}} \frac{\chi_\nu(t)\{1 - \chi_\nu(pt)\}}{t}\,\omega(t)\right\},$$

where $\nu = 1$ *or* 2 *and* $|\theta| \leqslant 1$.

Proof. By (3.8) and (3.5) we have

$$U_\nu(z) = \sum_{d|P(z)} \mu(d) \frac{\omega(d)}{d} \left(1 - \sum_{p|d} \{\chi_\nu((d, P_{p^+,z})) - \chi_\nu((d, P_{p,z}))\}\right)$$
$$= \sum_{d|P(z)} \frac{\omega(d)}{d} \left(\mu(d) + \sum_{p|d} \mu\left(\frac{d}{p}\right) \{\chi_\nu((d, P_{p^+,z})) - \chi_\nu((d, P_{p,z}))\}\right),$$

and if we now write $d = \delta p t$ where $\delta | P(p)$, $t | P_{p^+,z}$, we obtain

$$U_\nu(z) = V(z) + \sum_{p<z} \frac{\omega(p)}{p} \sum_{\delta|P(p)} \mu(\delta) \frac{\omega(\delta)}{\delta} \sum_{t|P_{p^+, z}} \mu(t) \frac{\chi_\nu(t) - \chi_\nu(pt)}{t}\,\omega(t)$$
$$= V(z)\left(1 + (-1)^{\nu-1} \sum_{p<z} \frac{\omega(p)}{p} \frac{1}{V(p, z)} \sum_{t|P_{p^+, z}} \chi_\nu(t)\{1 - \chi_\nu(pt)\} \frac{\omega(t)}{t}\right)$$

by (3.4). Note that the reciprocals of $V(p, z)$ are in order because (Ω_1) ensures that the numbers $\omega(p)/p$ are bounded away from 1. Since obviously

$$V(p, z) \geqslant V(z_n, z) \quad \text{if} \quad z_n \leqslant p < z_{n-1},$$

the result of the Lemma now follows at once on grouping the primes of $\mathscr{P}$ less than z into sub-sets corresponding to the intervals $[z_n, z_{n-1})$ $(n = 1, \dots, r)$.

There is, as Levin pointed out, considerable lattitude in the choice of the functions χ_ν (or, what amounts to the same thing, the sets D_ν); indeed, there is a choice which would lead to the powerful Rosser–Selberg sieve (see Selberg [10] or Iwaniec [4]). However, for our purpose Brun's choice suffices.

Let b be a positive integer. For $\nu = 1$ or 2, and each $n = 1, \dots, r$, put [5]

$$(3.10) \qquad \chi_\nu(d) = \begin{cases} 1 & \text{if} \quad \nu((d, P_{z_n, z})) \leqslant 2b - \nu + 2n - 1 \text{ for } n = 1, \dots, r, \\ 0 & \text{if} \quad d | P(z) \text{ otherwise.} \end{cases}$$

[5] It is here that the major misprint occurs in [1].

Then χ_1, χ_2 obviously satisfy (3.1) and (3.2). To check (3.3), suppose that $\chi_\nu(t) = 1$, $p < q(t)$ and $z_m \leqslant p < z_{m-1}$, say; then we need check (3.10) (with $d = pt$) only for $n = m$, that is, we have only to confirm that $\nu(pt) \leqslant 2b-\nu+2m-1$. But $\nu(t) \leqslant 2b-\nu+2m-1$; if also $\mu(t) = (-1)^{\nu(t)} = (-1)^r$, then $\nu(t) = 2b-\nu+2m-1$ is impossible. Hence $\nu(t) < 2b-\nu+ +2m-1$, and so $\nu(pt) \leqslant 2b-\nu+2m-1$. It then follows that $\chi_\nu(pt) = 1$, so that χ_1, χ_2 satisfy (3.3) too.

Let us now interpret the innermost sum (over t) on the right of Lemma 5 in the light of the choice (3.10). Here t makes a contribution to the sum only if $\chi_\nu(t) = 1$, $\chi_\nu(pt) = 0$. Since both t and pt divide $P_{z_n,z}$ it follows that $\nu(t) \leqslant 2b-\nu+2n-1$ and $\nu(pt) > 2b-\nu+2n-1$, so that $\nu(t) = 2b-\nu+2n-1$. Writing $pt = d$ and disregarding [6] all the other conditions on the prime decomposition of t arising from (3.10), we have, therefore, by Lemma 5 that

$$U_\nu(z) = V(z)\Bigg(1+\theta\sum_{n=1}^{r}\frac{1}{V(z_n, z)}\sum_{\substack{d\mid P_{z_n,z}\\ \nu(d)=2b-\nu+2n}}\frac{\omega(d)}{d}\Bigg), \qquad |\theta| \leqslant 1 \ (\nu = 1, 2).$$

We observe that the sum over d is the $(2b-\nu+2n)$th elementary symmetric function of the arguments $\omega(p)/p$, $z_n \leqslant p < z$, and so, by a well-known elementary inequality for such functions we arrive at

$$\text{(3.11)}\qquad U_\nu(z) = V(z)\Bigg(1+\theta\sum_{n=1}^{r}\frac{1}{V(z_n, z)}\,\frac{1}{(2b-\nu+2n)!}\Bigg\{\sum_{z_n\leqslant p<z}\frac{\omega(p)}{p}\Bigg\}^{2b-\nu+2n}\Bigg),$$
$$|\theta| \leqslant 1 \ (\nu = 1, 2).$$

So much for the leading terms in (3.7). As for the remainder terms, we have, by a simple combinatorial argument, that by virtue of (2.2)

$$\text{(3.12)}\qquad \big(\Omega_2(\varkappa)\big):\quad \sum_{d\mid P(z)}\chi_\nu(d)\,\omega(d)$$
$$\leqslant\Big(1+\sum_{p<z}\omega(p)\Big)^{2b-\nu+1}\prod_{n=1}^{r-1}\Big(1+\sum_{p<z_n}\omega(p)\Big)^2$$
$$\leqslant\big(1+A(2\operatorname{li}z+3)\big)^{2b-\nu+1}\prod_{n=1}^{r-1}\big(1+A(2\operatorname{li}z_n+3)\big)^2 \qquad (\nu = 1, 2).$$

[6] If these other conditions are retained, some form of combinatorial argument is required to take advantage of them. For $b = 1$ H. W. Hagedorn, of the University of Ulm, has succeeded in this by proving that if the j's are non-negative integers satisfying $j_1+\ldots+j_k \leqslant 2k-1$ $(k = 1, \ldots, n-1)$, $j_1+\ldots+j_n = 2n-1$, then

$$\sum\frac{1}{j_1!\ldots j_n!} = \frac{n^{2n-2}}{(2n-1)!} \qquad (n = 1, 2, \ldots).$$

To summarize the argument so far, we derive from (3.7), (3.11) and (3.12) that

$$\text{(3.13)}\qquad (\Omega_1), \big(\Omega_2(\varkappa)\big), (\mathrm{R}):\quad (-1)^r S(\mathscr{A}; \mathscr{P}, z)$$
$$\geqslant XV(z)\Bigg(1+\theta\sum_{n=1}^{r}\frac{V^{-1}(z_n, z)}{(2b-\nu+2n)!}\Bigg\{\sum_{z_n\leqslant p<z}\frac{\omega(p)}{p}\Bigg\}^{2b-\nu+2n}\Bigg) -$$
$$-K\big(1+A(2\operatorname{li}z+3)\big)^{2b-\nu+1}\prod_{n=1}^{r-1}\big(1+A(2\operatorname{li}z_n+3)\big)^2,$$
$$|\theta| \leqslant 1 \ (\nu = 1, 2).$$

To take matters further, one has to select a convenient partition (3.9). We shall see that a suitable choice leads to the following general result.

THEOREM 3 $(\Omega_1), \big(\Omega_2(\varkappa)\big), (\mathrm{R})$. *Let b be a positive integer, and let λ be a real number satisfying*

$$\text{(3.14)}\qquad 0 < \lambda e^{1+\lambda} < 1.$$

Then

$$\text{(3.15)}\qquad S(\mathscr{A}; \mathscr{P}, z)$$
$$\leqslant XV(z)\Bigg\{1+2\,\frac{\lambda^{2b+1}e^{2\lambda}}{1-\lambda^2e^{2+2\lambda}}\exp\Bigg((2b+3)\frac{B}{\lambda\log z}\Bigg)\Bigg\}+O\Big(Kz^{2b+\frac{2.01}{e^{2\lambda/\varkappa}-1}}\Big)$$

and

$$\text{(3.16)}\qquad S(\mathscr{A}; \mathscr{P}, z)$$
$$\geqslant XV(z)\Bigg\{1-2\,\frac{\lambda^{2b}e^{2\lambda}}{1-\lambda^2e^{2+2\lambda}}\exp\Bigg((2b+2)\frac{B}{\lambda\log z}\Bigg)\Bigg\}+O\Big(Kz^{2b-1+\frac{2.01}{e^{2\lambda/\varkappa}-1}}\Big)$$

where

$$B = \frac{A_2}{2}\Bigg\{1+A_1\Bigg(\varkappa+\frac{A_2}{\log 2}\Bigg)\Bigg\}.$$

The constants implied by the use of the O-notation do not depend on b and λ.

Proof. As in the proof of Theorem 2, we may suppose that z is large; otherwise we could apply Theorem 1. Accordingly we impose again the condition (2.14), with some suitably large constant B_1.

Let λ be a real number satisfying (3.14), and let us suppose that

$$\text{(3.17)}\qquad \frac{1}{V(z_n, z)} \leqslant e^{2(\lambda n+a)} \quad \text{for} \quad n = 1, \ldots, r,$$

where

$$a = \frac{B}{\log z};$$

the inequalities (3.17) have yet to be verified for some suitable choice of the numbers z_n in (3.9).

Then

$$\sum_{z_n\leqslant p<z}\frac{\omega(p)}{p}\leqslant\sum_{z_n\leqslant p<z}-\log\left(1-\frac{\omega(p)}{p}\right)=\log\frac{1}{V(z_n,z)}\leqslant 2(\lambda n+a)$$
$$\text{for } n=1,\ldots,r,$$

and it follows that

$$\sum_{n=1}^{r}\frac{V^{-1}(z_n,z)}{(2b-\nu+2n)!}\Big\{\sum_{z_n\leqslant p<z}\frac{\omega(p)}{p}\Big\}^{2b-\nu+2n}\leqslant\sum_{n=1}^{r}e^{2\lambda n+2a}\frac{(2\lambda n+2a)^{2b-\nu+2n}}{(2b-\nu+2n)!}$$
$$\leqslant e^{2a}(\lambda+a)^{2b-\nu}\sum_{n=1}^{r}\frac{(2ne^{-1})^{2n}}{(2n)!}\left(1+\frac{a}{\lambda n}\right)^{2n}(\lambda e^{1+\lambda})^{2n}$$

since $(2b-\nu+n)!\geqslant(2n)!(2n)^{2b-\nu}$. We observe that $\dfrac{(ne^{-1})^n}{n!}$ is decreasing and that $\left(1+\dfrac{a}{\lambda n}\right)^{2n}\leqslant e^{2a/\lambda}$. Hence the sum under consideration is at most

$$e^{2a}(\lambda+a)^{2b-\nu}2e^{-2}e^{2a/\lambda}\sum_{n=1}^{\infty}(\lambda e^{1+\lambda})^{2n}$$
$$=2\frac{\lambda^{2b-\nu+2}e^{2\lambda}}{1-\lambda^2e^{2+2\lambda}}\left(1+\frac{a}{\lambda}\right)^{2b-\nu}e^{2a\left(1+\frac{1}{\lambda}\right)}<2\frac{\lambda^{2b-\nu+2}e^{2\lambda}}{1-\lambda^2e^{2+2\lambda}}e^{(2b-\nu+4)\frac{a}{\lambda}}.$$

This, in view of (3.13), establishes the leading terms in (3.15) and (3.16); but a choice of the partition (3.9) justifying (3.17) has yet to be made.

We shall now choose (3.9). Let Δ be a positive real number and then define z_n by

$$(3.18)\qquad \log z_n=e^{-n\Delta}\log z\quad\text{for}\quad n=1,\ldots,r-1,\ z_r=2;$$

here, in order to satisfy (3.9), r is chosen so that

$$\log z_{r-1}=e^{-(r-1)\Delta}\log z>\log 2;$$

but $e^{-r\Delta}\log z\leqslant\log 2$, so that

$$(3.19)\qquad e^{(r-1)\Delta}<\frac{\log z}{\log 2}\leqslant e^{r\Delta}.$$

We shall now justify (3.17) subject to a suitable choice of Δ. Taking $w=z_n$ in (2.4) we deduce from (3.18) that

$$\frac{1}{V(z_n,z)}\leqslant\exp\left(n\Delta\varkappa+\frac{2Be^{n\Delta}}{\log z}\right)=e^{2a}\exp\left\{n\left(\Delta\varkappa+\frac{2B}{\log z}\,\frac{e^{n\Delta}-1}{n}\right)\right\},$$
$$n=1,\ldots,r,$$

(originally for $n=1,\ldots,r-1$ only, but, in view of (3.19), also for $n=r$). Since $\Delta>0$, we have

$$\frac{e^{n\Delta}-1}{n}\leqslant\frac{e^{r\Delta}-1}{r},$$

and the latter expression is by (3.19) at most

$$\Delta\frac{e^{r\Delta}}{r\Delta}\leqslant\Delta\frac{e^{\Delta}}{\log 2}\,\frac{\log z}{\log\left(\dfrac{\log z}{\log 2}\right)}.$$

Hence we obtain

$$\frac{1}{V(z_n,z)}\leqslant e^{2a}\exp\left\{n\Delta\varkappa\left(1+\frac{2Be^{\Delta}}{\varkappa\log 2}\,\frac{1}{\log\left(\dfrac{\log z}{\log 2}\right)}\right)\right\},\qquad n=1,\ldots,r;$$

and in view of (2.14) we meet the requirement (3.17) if we simply put

$$(3.20)\qquad \Delta=\frac{2\lambda}{\varkappa}\,\frac{1}{1+\varepsilon},\qquad \varepsilon=\frac{1}{200e^{1/\varkappa}},$$

(note that $\lambda\leqslant\frac{1}{2}$ by (3.14)).

Having established (3.17), we take the remainder terms in (3.13) one step further. With a suitable constant B_3 we have that

$$\big(1+\Delta(2\operatorname{li}z+3)\big)^{2b-\nu+1}\prod_{n=1}^{r-1}\big(1+\Delta(2\operatorname{li}z_n+3)\big)^2$$
$$\leqslant\left(B_3\frac{z}{\log z}\right)^{2b-\nu+1}\prod_{n=1}^{r-1}\left(B_3\frac{z_ne^{n\Delta}}{\log z}\right)^2,\qquad \nu=1,2.$$

But by (3.19), (3.20) and (2.14),

$$\prod_{n=1}^{r-1}\left(B_3\frac{e^{n\Delta}}{\log z}\right)=\left(B_3\frac{e^{r\Delta/2}}{\log z}\right)^{r-1}\leqslant\left(\frac{B_3e^{\Delta/2}}{\log z}\sqrt{\frac{\log z}{\log 2}}\right)^{r-1}<1;$$

and, by (3.18),

$$\prod_{n=1}^{r-1}z_n^2=\exp\Big\{2\log z\sum_{n=1}^{r-1}e^{-n\Delta}\Big\}\leqslant z^{2/(e^{\Delta}-1)}.$$

Hence

$$(3.21)\qquad \big(1+\Delta(2\operatorname{li}z+3)\big)^{2b-\nu+1}\prod_{n=1}^{r-1}\big(1+\Delta(2\operatorname{li}z_n+3)\big)^2$$
$$=O\big(z^{2b-\nu+1+2/(e^{\Delta}-1)}\big),\qquad \nu=1,2.$$

Finally, we shall deal with the exponent $2/(e^{\Lambda}-1)$ that occurs on the right of (3.21).

We have

$$e^{2\lambda/\varkappa}-e^{\Lambda}\leqslant\left(\frac{2\lambda}{\varkappa}-\Lambda\right)e^{2\lambda/\varkappa}\leqslant\varepsilon\Lambda e^{1/\varkappa},$$

so that, using $e^{\Lambda}-1\geqslant\Lambda$,

$$\frac{e^{2\lambda/\varkappa}-1}{e^{\Lambda}-1}\leqslant 1+\frac{\varepsilon\Lambda e^{1/\varkappa}}{e^{\Lambda}-1}\leqslant 1+\varepsilon e^{1/\varkappa}=\frac{2.01}{2}.$$

Thus

$$\frac{2}{e^{\Lambda}-1}\leqslant\frac{2.01}{e^{2\lambda/\varkappa}-1},$$

and if we insert this in (3.21), we see that the proof of Theorem 3 is now complete.

4. The principal Fundamental Lemma. We shall now deduce from Theorem 3 a Fundamental Lemma of high quality, which yields the asymptotic relation (1.1) subject only to the condition

$$\frac{\log X}{\log z}\to\infty\quad\text{as } X\to\infty,$$

and which is also very precise in the sense explained in Section 1.

THEOREM 4 (Ω_1), $(\Omega_2(\varkappa))$, (R). *Let* $X\geqslant z$ *and write*

$$u=\frac{\log X}{\log z}.$$

Then

$$S(\mathscr{A};\mathscr{P},z)=XV(z)\{1+O(e^{-u(\log u-\log\log 3u-\log\varkappa-2)})+O(Ke^{-\sqrt{\log X}})\},$$

where the O-constants depend at most on $\varkappa$, A_1 *and* A_2.

Proof. Suppose first that

$$u\geqslant B_4=B_4(\varkappa,A_1,A_2),$$

where B_4 is a sufficiently large constant. In view of Theorem 2 and (2.5) we may assume that

$$\log z>u.$$

Now apply Theorem 3 with

$$b=\left[\frac{u}{2}-\frac{u}{2\log u}\right]\quad\text{and}\quad\lambda=\frac{e\varkappa\log u}{u};$$

inequalities (3.15) and (3.16) together yield, in view of (2.5)

$$(4.1)\qquad S(\mathscr{A};\mathscr{P},z)=XV(z)\left\{1+O\left(\exp\left\{-2b\log\frac{1}{\lambda}+2b\frac{B}{\lambda\log z}\right\}\right)+\right.$$
$$\left.+O\left(K\exp\left\{-\log z\left(u-2b-\frac{e\varkappa}{2\lambda}\right)+\varkappa\log\log z\right\}\right)\right\}.$$

Using that $\log z>u$, the error terms are

$$O\left(\exp\left\{-\left(u-\frac{u}{\log u}\right)\log\left(\frac{u}{e\varkappa\log u}\right)+O\left(\frac{u}{\log u}\right)\right\}\right)+$$
$$+O\left(K\exp\left\{-\log z\frac{u}{2\log u}+\varkappa\log\log z\right\}\right)$$
$$=O\left(\exp\{-u(\log u-\log\log u-\log\varkappa-2)\}\right)+O(Ke^{-\sqrt{\log X}})$$

and our theorem follows at once from (4.1) if $u\geqslant B_4$.

If $1\leqslant u<B_4$, we have, by virtue of the definition of the sifting function S, that since $z=X^{1/u}$,

$$S(\mathscr{A};\mathscr{P},z)\leqslant S(\mathscr{A};\mathscr{P},X^{1/B_4}).$$

We now apply the preceding result (with $u=B_4$) to the expression on the right, and obtain

$$S(\mathscr{A};\mathscr{P},z)\leqslant XV(X^{1/B_4})\{O(1)+O(Ke^{-\sqrt{\log X}})\}.$$

Hence, using (2.4) (note that we may assume $X>2^{B_4}$), we arrive at

$$S(\mathscr{A};\mathscr{P},z)\leqslant XV(z)\{O(1)+O(Ke^{-\sqrt{\log X}})\}.$$

Since, trivially, $S\geqslant 0$, this completes the proof of the Theorem for $u\geqslant 1$.

Condition $u\geqslant 1$ is equivalent to $X\geqslant z$; it is clear from the last stage of the foregoing proof that this condition may be weakened, or again that it could be replaced by a stronger condition.

For u bounded (and $K\ll e^{\sqrt{\log X}}$), the theorem tells us that

$$S(\mathscr{A};\mathscr{P},z)=O(XV(z)),$$

which is often useful in situations where the sieve is used in an auxiliary capacity; indeed, this is just the result that is usually required when one encounters the phrase "by Brun's sieve ..." in the literature.

5. Applications of Theorem 4. The Fundamental Lemma has important applications in those problems where one needs precise information about the distribution of numbers (belonging to some arithmetical sequence) which have no small prime factors. For example, such problems arise in the study of additive arithmetic functions (see Kubilius [5], especially the Fundamental Lemmas given in Chapter 1; see also W. Philipp [9], Lemma 5.1.1 and a forthcoming improvement).

We shall illustrate the effectiveness of Theorem 4 by proving, in conclusion, the following general result.

THEOREM 5. *Let $f_1(n), \ldots, f_g(n)$ be distinct irreducible polynomials with integer coefficients, and write*

$$F(n) = f_1(n) \ldots f_g(n).$$

Let $\varrho(p)$ denote the number of solutions of the congruence

$$F(n) \equiv 0 \bmod p,$$

and assume that

$$\varrho(p) < p \quad \textit{for all primes } p. \tag{5.1}$$

Let u and x be real numbers such that $u \geqslant 1$ and $x^{1/u} \geqslant 2$; and let $q = q(x, u)$ (with or without suffices) denote a number having no prime divisors less than $x^{1/u}$. Then

$$\begin{aligned}(5.2)\qquad &|\{n\colon 1 \leqslant n \leqslant x, f_i(n) = q_i;\ \textit{for}\ i = 1, \ldots, g\}| \\ &= x \prod_{p<x^{1/u}} \left(1 - \frac{\varrho(p)}{p}\right) \{1 + O_F(e^{-u(\log u - \log\log 3u - \log g - 2)}) + O_F(e^{-\sqrt{\log x}})\}.\end{aligned}$$

Moreover, we have also that

$$\begin{aligned}(5.3)\qquad &|\{n\colon 1 \leqslant n \leqslant x, f_i(n) = q_i\ \textit{for}\ i = 1, \ldots, g\}| \\ &= (ue^{-\gamma})^g \prod_p \left(1 - \frac{\varrho(p)-1}{p-1}\right)\left(1 - \frac{1}{p}\right)^{-g+1} \times \\ &\qquad \times \frac{x}{\log^g x} \left\{1 + O_F(e^{-u(\log u - \log\log 3u - \log g - 2)}) + O_F\left(\frac{u}{\log x}\right)\right\},\end{aligned}$$

where all the O_F-constants may depend on the coefficients and degrees of $f_1, \ldots, f_g$.

Although we have not explicitly required the polynomials f_i to have positive degrees, the theorem is, in fact, of interest when this is the case; for if one of the f_i's had zero degree, then, by (5.1), it would have to be equal to ± 1.

Proof. We take as the sequence to be sifted

$$\mathscr{A} = \{F(n)\colon 1 \leqslant n \leqslant x\},$$

and as $\mathscr{P}$ the set $\mathscr{P}_1$ of all primes. Denote by $\varrho(d) = \varrho_F(d)$ the number of solutions of the congruence

$$F(n) \equiv 0 \bmod d \cdot$$

it is well-known that ϱ is a multiplicative function, so that

$$\varrho(d) = \prod_{p|d} \varrho(p) \quad \text{if} \quad \mu(d) \neq 0.$$

We find that

$$\sum_{\substack{a \in \mathscr{A} \\ a \equiv 0 \bmod d}} 1 = |\{n\colon 1 \leqslant n \leqslant x, F(n) \equiv 0 \bmod d\}| = \varrho(d)\left(\frac{x}{d} + \theta\right), \tag{5.4}$$
$$|\theta| \leqslant 1;$$

accordingly, and with a view to applying Theorem 4, we choose

$$X = x, \qquad \omega(d) = \varrho(d)$$

(note that $\overline{\mathscr{P}}$ is empty), and it then follows from (5.4) that

$$|R_d| \leqslant \omega(d).$$

Hence condition (R) is satisfied with $K = 1$. The arithmetic function ϱ is, except in special circumstances, non-elementary in the sense that individual numbers $\varrho(d)$ are hard, or even impossible to determine. However, we know from Lagrange's theorem that $\varrho(p) = p$ or $\varrho(p) \leqslant G$; hence, if F has no fixed prime divisors — which is equivalent to saying, if F satisfies (5.1) — we have

$$\varrho(p) \leqslant \min(p-1, G), \qquad G = \deg F. \tag{5.5}$$

It follows by distinguishing between primes $\leqslant G$ and primes $> G$, that condition (Ω_1) is satisfied with $A_1 = G+1$.

Next, let $\varrho^{(i)}(p)$ denote the number of solutions of $f_i(n) \equiv 0 \bmod p$, for $i = 1, \ldots, g$; then

$$\sum_{p<w} \frac{\varrho^{(i)}(p)}{p} \log p = \log w + O_F(1)$$

(cf. Nagell [8]) and for all but at most $O_F(1)$ primes we have

$$\varrho_F(p) = \varrho^{(1)}(p) + \ldots + \varrho^{(g)}(p).$$

Hence

$$\sum_{w \leqslant p < z} \frac{\varrho_F(p)}{p} \log p - g \log \frac{z}{w} = O_F(1),$$

so that $(\Omega_2(\varkappa))$ is satisfied with $\varkappa = g$ and $A_2 = O_F(1)$. We may now apply Theorem 4 with $z = x^{1/u}$; and we obtain (5.2) at once.

Next, it follows from [2] (Lemma 2, (2.12); see condition (Ω_2) on p. 244), that

$$\prod_{p<x^{1/u}}\left(1-\frac{\varrho(p)}{p}\right)=\prod_{p}\left(1-\frac{\varrho(p)}{p}\right)\left(1-\frac{1}{p}\right)^{-g}\frac{e^{-\gamma g}u^g}{\log^g x}\left\{1+O_F\left(\frac{u}{\log x}\right)\right\}$$

where the infinite product is convergent. Finally, the identity

$$\frac{1-\dfrac{\varrho(p)}{p}}{1-\dfrac{1}{p}}=1-\frac{\varrho(p)-1}{p-1}$$

completes the proof of (5.3).

It is worth remarking that the condition

$$(\Omega_0)\qquad\qquad \omega(p)\leqslant A_0,\quad A_0\geqslant 1,$$

implies $(\Omega_2(\varkappa))$ with $\varkappa=A_2=A_0$. In particular, in the case of Theorem 5, we infer from (5.5) that (Ω_0) holds with $A_0=G$. Hence (5.2) is also true if, in the first O-term g is replaced by G; and then, because we may now take $A_2=G$ both the O-constants in (5.2) depend at most on G. A similar remark applies in (5.3), but only to the first O-term.

An interesting special case of this general result corresponds to the choice of the f_i as linear polynomials whose product has no fixed prime divisors. Such results are sometimes interpreted, somewhat optimistically, in terms of so called 'quasi-primes' (cf. e.g. Lavrik [6]) and the reader who wishes to follow up this connection should have little difficulty in deriving from Theorem 4 and 5, for instance the quasi-prime analogues of the Goldbach and prime-twin problems.

The result corresponding to Theorem 5 for $\mathscr{A}=\{F(p)\colon p\leqslant x\}$ cannot be derived from Theorem 4; the reason is that Brun's sieve as given in Theorem 3 uses an inadequate (for this purpose) form (R) of a remainder condition. We shall return to an even more comprehensive Brun's sieve in another paper.

References

[1] H. Halberstam and H.-E. Richert, *A new look at Brun's sieve*, Bull. Soc. Math. France 25 (1971), pp. 97–106.

[2] — — *Mean value theorems for a class of arithmetic functions*, Acta Arith. 18 (1971), pp. 243–256.

[3] C. Hooley, *On the representation of a number as the sum of two squares and a prime*, Acta Math. 97 (1957), pp. 189–210.

[4] H. Iwaniec, *On the error term in the linear sieve*, Acta Arith. 19 (1971), pp. 1–30.

[5] J. Kubilius, *Probabilistic Methods in the Theory of Numbers* (AMS Translations of Math. Monographs, Vol. II, 1964).

[6] A. F. Lavrik, *The theory of quasiprime numbers*, Sov. Math. 4 (1963), pp. 1355–1359.

[7] Б. В. Левин, *Сравнение решений А. Сельберга и В. Бруна*, УМН 20 (5) (125) (1965), pp. 214–220.

[8] T. Nagell, *Généralisation d'un théorème de Tchebycheff*, Journal de Mathématiques (8) 4 (1921), pp. 343–356.

[9] W. Philipp, *Mixing sequences of random variables and probabilistic number theory*, Mem. Amer. Math. Soc. 114 (1971), pp. 1–102.

[10] A. Selberg, *Sieve Methods*, Proc. Symposia in Pure Mathematics 20 (1971), pp. 311–351.

Received on 18. 7. 1972 (308)