

References

- [1] S. L. G. Choi, *Estimation of the largest number of distinct products from two sets of integers*, to appear.
- [2] Т. А. Фрейман, *Начала структурной теории сложения множества (Concerning general regularities of the additive theory of numbers)*, Казань 1966.
- [3] E. Szemerédi, *On sets of integers containing no four elements in arithmetic progression*, Acta Math. Acad. Sci. Hungar. 20 (1969), pp. 89–104.
- [4] P. Varnavides, *On certain sets of positive density*, Journ. London Math. Soc. 34 (1959), pp. 358–360.

Received on 3. 4. 1973

(390)

Brun's method and the Fundamental Lemma, II*

by

H. HALBERSTAM (Nottingham) and H.-E. RICHERT (Ulm)

To the memory of Yu. V. Linnik

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

$$P(z) = \prod_{\substack{p < z \\ p \in \mathfrak{P}}} p, \quad P_{w,z} = P(z)/P(w)$$

and

$$S(\mathfrak{A}; \mathfrak{P}, z) = |\{a \in \mathfrak{A}, (a, P(z)) = 1\}|,$$

where $|\{\dots\}|$ denotes the cardinality of the set $\{\dots\}$.

Let $\omega(d)$ be a non-negative multiplicative arithmetic function on the sequence of square-free integers d which satisfies the following conditions:

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

there exists a constant $A_1 \geq 1$ such that

$$(\Omega_1) \quad \frac{\omega(p)}{p} \leq 1 - \frac{1}{A_1};$$

there exist constants $\varkappa > 0$ and $A_2 \geq 1$ such that

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

* This paper is a sequel to [1]. A brief announcement of its results was contained in [2].

We shall write

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

We postulate the existence of a real number $X > 1$ and an arithmetic function ω of the above class such that the 'remainders'

$$R_a := \sum_{\substack{d \in \mathfrak{A} \\ a \equiv 0 \pmod{d}}} 1 - \frac{\omega(d)}{d} X$$

are small on average, in a sense to be made precise in the next section. In an earlier paper bearing the same title (see [1]) we established a general form of Brun's sieve, and derived from it a rather sharp Fundamental Lemma (that is, an asymptotic formula for $S(\mathfrak{A}; \mathfrak{P}, z)/(XV(z))$ valid in an extensive region of the $X-z$ plane) under the hypothesis (Ω_1) , $(\Omega_2(x))$ and

$$(R) \quad |R_d| \leq K\omega(d) \quad \text{if} \quad \mu(d) \neq 0, (d, \mathfrak{P}) = 1,$$

for some real number $K \geq 1$. In this note we shall replace (R) by a much cruder upper bound condition together with an 'average' condition of Bombieri type (cf. condition $(R(x, a))$ in [3] or [4]); and we shall indicate how the method of [1] leads, with very little modification, to an even more general form of Brun's sieve. We shall derive from this form a new Fundamental Lemma, and we shall apply this, by way of illustration, to prove the following companion result, for polynomial sequences with prime arguments, of Theorem 5 of [1]:

THEOREM 1. *Let $f_1(n), \dots, f_g(n)$ be distinct irreducible polynomials with integer coefficients, and suppose that*

$$(1.1) \quad f_i(n) \neq \pm n \quad (i = 1, \dots, g).$$

Write $F(n) = f_1(n) \dots f_g(n)$, let k denote the degree of F , and let $\varrho(p) = \varrho_F(p)$ be the number of solutions of the congruence

$$F(n) \equiv 0 \pmod{p}, \quad 0 \leq n < p.$$

Assume that

$$(1.2) \quad \varrho(p) < p \quad \text{for all primes } p$$

and that

$$(1.3) \quad \varrho(p) < p-1 \quad \text{if} \quad p \nmid F(0),$$

and define

$$(1.4) \quad \varrho'(p) = \begin{cases} \varrho(p) - 1, & p \mid F(0), \\ \varrho(p), & p \nmid F(0). \end{cases}$$

Let v and x be real numbers such that $v \geq 3$ and $x^{1/v} \geq 2$; and let $q = q(x, v)$ (with or without suffices) denote a number (usually referred to as a quasi-prime) having no prime factor less than $x^{1/v}$. Then we have

$$(1.5) \quad \left\{ \{p: p \leq x, f_i(p) = q_i \text{ for } i = 1, \dots, g\} \right\} \\ = (li \ x) \prod_{p < x^{1/v}} \left(1 - \frac{\varrho'(p)}{p-1}\right) \left\{ 1 + O_F(e^{-1v(\log v - \log \log 2v - \log 3v - 2)}) + O_F\left(\frac{1}{\log x}\right) \right\};$$

moreover, the expression on the right is equal to

$$(ve^{-v})^g \prod_p \left(1 - \frac{\varrho'(p)+1}{p}\right) \left(1 - \frac{1}{p}\right)^{-g-1} \left(\frac{x}{\log^{g+1} x}\right) \times \\ \times \left\{ 1 + O_F(e^{-1v(\log v - \log \log 2v - \log 3v - 2)}) + O_F\left(\frac{v}{\log x}\right) \right\}.$$

2. Brun's sieve. It will serve us best to begin with a statement of the form of Brun's sieve that is implicit in [1], in which the remainders R_a are still explicit and which is therefore free of the condition (R).

THEOREM 2 (Ω_1) , $(\Omega_2(x))$: *Let b be a positive integer, let λ be a real number satisfying*

$$(2.1) \quad 0 < \lambda e^{1+\lambda} < 1,$$

and let

$$(2.2) \quad B = \frac{1}{2} A_2 \left\{ 1 + A_1 \left(x + \frac{A_2}{\log 2} \right) \right\}.$$

Define

$$(2.3) \quad A = \frac{2\lambda}{x} \cdot \frac{1}{1+\varepsilon}, \quad \varepsilon = \frac{1}{200e^{1/\lambda}},$$

and let the sequence

$$2 = z_r < z_{r-1} < \dots < z_1 < z$$

be given by

$$(2.4) \quad \log z_n = e^{-nA} \log z \quad (n = 1, \dots, r-1).$$

For $v = 1$ or 2 , for each $n = 1, \dots, r$ and for each positive divisor d of $P(z)$ put

$$(2.5) \quad \chi_v(d) = \begin{cases} 1 & \text{if } \nu((d, P_{z_n, z})) \leq 2b - v + 2n - 1 \text{ for } n = 1, \dots, r, \\ 0 & \text{if } d \mid P(z) \text{ otherwise.} \end{cases}$$

Then

$$(2.6) \quad S(\mathfrak{A}; \mathfrak{P}, z) \leq XV(z) \left\{ 1 + 2 \frac{\lambda^{2b+1} e^{2\lambda}}{1 - \lambda^2 e^{2+2\lambda}} \exp\left((2b+3) \frac{B}{\lambda \log z}\right) \right\} + \\ + \sum_{d \mid P(z)} \chi_1(d) |R_d|$$

(¹) Throughout, $\nu(n)$ denotes the number of prime factors of n .

and

$$(2.7) \quad S(\mathfrak{A}; \mathfrak{P}, z) \geq XV(z) \left\{ 1 - 2 \frac{\lambda^{2b} e^{2\lambda}}{1 - \lambda^2 e^{2+2\lambda}} \exp \left((2b+2) \frac{B}{\lambda \log z} \right) \right\} - \sum_{d|P(z)} \chi_2(d) |R_d|;$$

moreover, for any constant $A \geq 1$, we have

$$(2.8) \quad \sum_{d|P(z)} \chi_r(d) A^{v(d)} = O(z^{2b+1-\nu+\frac{2.01}{e^{2\lambda/\kappa}-1}}),$$

where the implied O -constant, while it may depend on A_1, A_2, κ and A , does not depend on b and λ .

We now introduce in place of (R) a pair of new conditions on the remainders R_d . We shall suppose first that there exist a real number $K \geq 1$ and a constant $A_0 \geq 1$ such that

$$(R_0) \quad |R_d| \leq K \left(\frac{X \log X}{d} + 1 \right) A_0^{v(d)} \quad \text{for} \quad \mu(d) \neq 0, (d, \mathfrak{P}) = 1;$$

and we shall suppose also that for some constant α ($0 < \alpha \leq 1$) there exist corresponding to any given constant $C \geq 1$ constants $C_0 \geq 1$ and $C_1 \geq 1$ such that

$$(R_1(\kappa, \alpha)) \quad \sum_{\substack{d < X^{\alpha \log^{-C_0} X} \\ (d, \mathfrak{P}) = 1}} \mu^2(d) |R_d| \leq C_1 \frac{X}{\log^{\kappa+C} X}.$$

It is clear that (R_0) is, in general, much weaker than (R) (take, for example, the common case when $\omega(p) \leq A_0$ for all p), and that (R) implies a condition of type $(R_1(\kappa, 1))$. We shall see in Section 4 that both conditions are satisfied in the case of Theorem 1.

We shall now apply the new conditions (R_0) and $(R_1(\kappa, \alpha))$ in conjunction with (2.8) to the remainder terms in (2.6) and (2.7): we have, for $\nu = 1$ and 2 that

$$\begin{aligned} \sum_{d|P(z)} \chi_r(d) |R_d| &\leq \sum_{\substack{d < X^{\alpha \log^{-C_0} X} \\ (d, \mathfrak{P}) = 1}} |R_d| + K \sum_{\substack{d|P(z) \\ d > X^{\alpha \log^{-C_0} X}}} \left(\frac{X \log X}{d} + 1 \right) A_0^{v(d)} \chi_r(d) \\ &\leq C_1 \frac{X}{\log^{\kappa+C} X} + 2KX^{1-\alpha} \log^{C_0+1} X \sum_{d|P(z)} A_0^{v(d)} \chi_r(d) \\ &= O \left(\frac{X}{\log^{\kappa+C} X} + KX^{1-\alpha} z^{2b+1-\nu+\frac{2.01}{e^{2\lambda/\kappa}-1}} \log^{C_0+1} X \right). \end{aligned}$$

If now we adopt the convenient notation

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

and if also we recall from [1] (inequality (2.5)) that

$$(2.9) \quad 1/V(z) = O(\log^{\kappa} z),$$

we arrive at the estimates

$$(2.10) \quad \sum_{d|P(z)} \chi_r(d) |R_d| \leq XV(z) \left\{ \frac{u^{-\kappa}}{\log^C X} + Kz^{-\alpha u+2b+1-\nu+\frac{2.01}{e^{2\lambda/\kappa}-1}} u^{C_0+1} \log^{C_0+\kappa+1} z \right\};$$

($\nu = 1, 2$).

From Theorem 2 and (2.10) we now obtain

THEOREM 3 (Ω_1), ($\Omega_2(\kappa)$), (R_0) , $(R_1(\kappa, \alpha))$: Let b be a positive integer, let λ be a real number satisfying (2.1), let B be as defined in (2.2) and write

$$(2.11) \quad u = \log X / \log z.$$

Then

$$(2.12) \quad \frac{S(\mathfrak{A}; \mathfrak{P}, z)}{XV(z)} \leq 1 + 2 \frac{\lambda^{2b+1} e^{2\lambda}}{1 - \lambda^2 e^{2+2\lambda}} \exp \left((2b+3) \frac{B}{\lambda \log z} \right) + O(Kz^{-\alpha u+2b+\frac{2.01}{e^{2\lambda/\kappa}-1}} u^{C_0+1} \log^{C_0+\kappa+1} z) + O(u^{-\kappa} \log^{-C} X)$$

and

$$(2.13) \quad \frac{S(\mathfrak{A}; \mathfrak{P}, z)}{XV(z)} \geq 1 - 2 \frac{\lambda^{2b} e^{2\lambda}}{1 - \lambda^2 e^{2+2\lambda}} \exp \left((2b+2) \frac{B}{\lambda \log z} \right) + O(Kz^{-\alpha u+2b-1+\frac{2.01}{e^{2\lambda/\kappa}-1}} u^{C_0+1} \log^{C_0+\kappa+1} z) + O(u^{-\kappa} \log^{-C} X),$$

where the O -constants, while they may depend on $A_0, A_1, A_2, \kappa, \alpha$ and C , do not depend on λ or b .

To illustrate the effectiveness of Theorem 3, let us apply it to the 'prime twins' problem. We take $\mathfrak{A} = \{p+2: p \leq x\}$ and $\mathfrak{P} = \{p: p > 2\}$, so that $\mathfrak{P} = \{2\}$. Then if d is square-free and odd,

$$\sum_{\substack{a \in \mathfrak{A} \\ a \equiv 0 \pmod{d}}} 1 = \sum_{\substack{p \leq x \\ p \equiv -2 \pmod{d}}} 1 = \pi(x; d, -2) = \frac{\text{li } x}{\varphi(d)} + R_d;$$

accordingly we take $X = \text{li } x$, $\omega(p) = 0$ if $p = 2$ and $\omega(p) = \frac{p}{p-1}$ if p is odd, and we find that (Ω_1) is then satisfied with $A_1 = 2$, $(\Omega_2(\kappa))$ with

$z = 1 = A_2, (R_0)$ with $K = 2$ and $A_0 = 1$, and $(R_1(1, \alpha))$ holds with $\alpha = \frac{1}{2}$ (and $C_0 = C + 13$) by virtue of Bombieri's theorem (for the version used here, see Montgomery [5]). With this choice of parameters we take $b = 1$ in (2.13) and obtain (note that now $B < 2$ by (2.2))

$$(2.14) \quad \frac{S(\mathfrak{A}; \mathfrak{P}, z)}{XV(z)} \geq 1 - 2 \frac{\lambda^2 e^{2\lambda}}{1 - \lambda^2 e^{2+2\lambda}} \exp\left(\frac{8}{\lambda \log z}\right) + O(z^{-1+u+1+\frac{2.01}{e^{2\lambda}-1}} u^{C+14} \log^{15+C} z) + O(u^{-1} \log^{-C} X).$$

To ensure that the right hand side is positive for all large enough values of x we must choose positive numerical values for λ and u so that

$$(2.15) \quad 1 - \frac{2\lambda^2 e^{2\lambda}}{1 - \lambda^2 e^{2+2\lambda}} > 0$$

(of course, (2.1) must hold too!) and

$$(2.16) \quad u > 2 + \frac{4.02}{e^{2\lambda} - 1};$$

the quality of our result will depend on choosing u as small as possible, and therefore λ as large as possible. The choice $e^\lambda = 1.288$ just satisfies (2.15) and (easily) (2.1); and when substituted in (2.16) permits a choice of $u < 9$. It follows at once that $p+2$ is infinitely often a number having at most eight prime factors (counted according to multiplicity).

Actually, it is clear from the proof of Theorem 3 of [1] that our estimates for $S(\mathfrak{A}; \mathfrak{P}, z)$ can be improved by separating the term corresponding to $n = 1$ before embarking upon the various approximations that lead to the relatively simple forms (2.6) and (2.7) above (see the calculations following (3.17) in [1]) — this is the usual procedure in most classical formulations of Brun's sieve. In particular, the first two terms on the right of (2.14) can be replaced by, essentially

$$1 - 2\lambda^2 e^{2\lambda} \left(1 + \frac{16}{3} \frac{\lambda^2 e^{2\lambda}}{1 - \lambda^2 e^{2+2\lambda}}\right)$$

(we may ignore the exponential term in this application, as we did earlier, because λ is a numerical constant and $z = X^{1/u}$ is therefore large) and this expression exceeds 0.04 with the choice $e^\lambda = 1.293$. Now this choice satisfies (2.1) and allows us to select a value of u satisfying (2.16) which is less than 8. Hence we may conclude that $p+2$ is infinitely often a number having at most seven prime factors (counted according to multiplicity).

The refinement indicated in the second footnote in Section 3 of [1], possibly combined with a weighting procedure (see [4]), should lead to further improvement.

3. A Fundamental Lemma. We may now deduce from Theorem 3

THEOREM 4 $(\Omega_1), (\Omega_2(\kappa)), (R_0), (R_1(\kappa, \alpha))$: Let $X \geq z$ and write

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

Then

$$S(\mathfrak{A}; \mathfrak{P}, z) = XV(z) \{1 + O(e^{-\alpha u (\log u - \log \log 3u - \log(\kappa/\alpha) - 2)}) + O(K \log^{-C} X)\},$$

where the O -constants depend at most on $A_0, A_1, A_2, \kappa, \alpha$ and C .

Proof. We follow the argument of the proof of Theorem 4 of [1]. The result is of interest only if $u \rightarrow +\infty$, and we concentrate therefore on the case of u large (although we can deal also with small u as in [1]).

For $u \geq \log z$, that is to say, for $\log z \leq \sqrt{\log X}$, we can easily check that the analogues of Theorems 1 and 2 of [1] are respectively

$$(\Omega_1), (\Omega_2(\kappa)), (R_0), (R_1(\kappa, \alpha)):$$

$$S(\mathfrak{A}; \mathfrak{P}, z) = XV(z) \{1 + O(\log^{-C} X) + O(KX^{-\alpha} \log^{C_0+\kappa} X \cdot (1 + A_0)^{\kappa(z)})\}$$

and

$$(\Omega_1), (\Omega_2(\kappa)), (R_0), (R_1(\kappa, \alpha)):$$

$$S(\mathfrak{A}; \mathfrak{P}, z) = XV(z) \{1 + O(\log^{-C} X)\} + O(KX^{1-\frac{\alpha}{2}} \log^{C_0} X);$$

and that both these are better, in their limited ranges of effectiveness, than the stated result.

This allows us to suppose that

$$u < \log z,$$

and here an application of Theorem 3 with

$$b = \left[\frac{\alpha}{2} u - \frac{\alpha}{2} \frac{u}{\log u} \right], \quad \lambda = \frac{e\kappa}{\alpha} \frac{\log u}{u}$$

leads readily to the result.

4. Proof of Theorem 1. We take \mathfrak{A} to be the sequence $\{F(p) : p \leq x\}$ and \mathfrak{P} to be the set \mathfrak{P}_1 of all primes. Then, if $\mu(d) \neq 0$,

$$\begin{aligned} \sum_{\substack{a \in \mathfrak{A} \\ a \equiv 0 \pmod{d}}} 1 &= |\{p : p \leq x, F(p) \equiv 0 \pmod{d}\}| = \sum_{l=1}^d \sum_{\substack{p \leq x \\ p \equiv l \pmod{d} \\ F(p) \equiv 0 \pmod{d}}} 1 \\ &= \sum_{\substack{l=1 \\ F(l) \equiv 0 \pmod{d}}}^d \pi(x; d, l) = \sum_{\substack{l=1 \\ (l, d) = 1 \\ F(l) \equiv 0 \pmod{d}}}^d \pi(x; d, l) + \theta_e(d), \end{aligned}$$

$$0 \leq \theta \leq 1;$$

writing

$$E(x; d, l) = \pi(x; d, l) - \frac{\text{li } x}{\varphi(d)},$$

we obtain

$$\sum_{\substack{\alpha \in \mathbb{X} \\ \alpha \equiv 0 \pmod{d}}} 1 = \frac{\text{li } x}{\varphi(d)} \varrho'(d) + \sum_{\substack{l=1 \\ (l, d)=1 \\ F(l) \equiv 0 \pmod{d}}}^d E(x; d, l) + \theta \varrho(d) \\ = \frac{\text{li } x}{d} \cdot \frac{d \varrho'(d)}{\varphi(d)} + \theta \varrho(d) \{E(x, d) + 1\}, \quad |\theta| \leq 1,$$

where $\varrho'(d)$ is the number of solutions of

$$F(n) \equiv 0 \pmod{d}, \quad 0 \leq n < d, \quad (n, d) = 1,$$

so that $\varrho'(d) \leq \varrho(d)$, $\varrho'(p)$ satisfies (1.4), and where

$$E(x; d) = \max_{\substack{1 \leq l \leq d \\ (l, d)=1}} |E(x; d, l)|.$$

It is not hard to prove that ϱ' is a multiplication function, and therefore an appropriate choice of X and ω here is

$$(4.1) \quad X = \text{li } x, \quad \omega(d) = \frac{d \varrho'(d)}{\varphi(d)};$$

we may clearly assume that $X > 1$. It follows that

$$(4.2) \quad |R_d| \leq \{E(x, d) + 1\} \varrho(d).$$

In order to apply Theorem 4, we must check that the basic conditions are satisfied. From a well known elementary result we know that

$$\varrho(p) \leq k$$

whenever $\varrho(p) < p$, whence, by (1.4),

$$\frac{\omega(p)}{p} = \frac{\varrho'(p)}{p-1} \leq 1 - \frac{1}{k+1} \quad \text{for all } p;$$

hence (Ω_1) holds with $A_1 = k+1$. Next, $(\Omega_2(\kappa))$ is satisfied with $\kappa = g$ and $A_2 = O_F(1)$ by virtue of a classical result of Nagell [6] (see the proofs of Theorems 4 and 6 in [4]). We come to verify (R_0) and $(R_1(\kappa, \alpha))$, and here we base ourselves on (4.2). Since $\varrho(d) \leq k^{v(d)}$ for square-free d , the second

of these two conditions follows from (4.2) by Bombieri's theorem (as is demonstrated in full detail in the proof of Theorem 6 of [4]), with $\kappa = g$, $\alpha = \frac{1}{2}$ and taking (as we may do) $C = 1$. As for the first condition, we have

$$|R_d| \leq \{E(x, d) + 1\} k^{v(d)} \leq \left\{ \frac{x}{d} + 2 \right\} k^{v(d)} \leq 2 \left\{ \frac{X \log X}{d} + 1 \right\} k^{v(d)},$$

so that (R_0) holds with $K = 2$ and $A_0 = k$.

We may therefore apply Theorem 4. Here we take $z = x^{1/v}$, so that by (4.1) and because $x \geq 2^v \geq 8$ by hypothesis,

$$u = \frac{\log X}{\log z} = v \frac{\log(\text{li } x)}{\log x} \geq v \frac{\log(x/\log x)}{\log x} = v \left(1 - \frac{\log \log x}{\log x} \right) \geq \frac{2}{3} v;$$

hence, by (4.1) again, (1.5) follows at once from Theorem 4.

As for the last statement in the theorem, we have

$$1 - \frac{\varrho'(p)}{p-1} = \left(1 - \frac{1}{p} \right)^{-1} \left(1 - \frac{\varrho'(p)+1}{p} \right),$$

and therefore the product on the right of (1.5) is equal to (see [3], Lemma 2, (2.12), noting that condition (Ω_2) on p. 244 with $\omega(p) = \varrho'(p) + 1$ is satisfied with $\kappa = g+1$ and $A_2 = O_F(1)$, $L = O_F(1)$)

$$\prod_p \left(1 - \frac{\varrho'(p)+1}{p} \right) \left(1 - \frac{1}{p} \right)^{-g-1} \frac{e^{-\gamma g} u^g}{\log^g x} \left\{ 1 + O_F \left(\frac{u}{\log x} \right) \right\};$$

this completes the proof of Theorem 1.

References

- [1] H. Halberstam and H.-E. Richert, *Brun's method and the Fundamental Lemma*, Acta Arith. 24 (1973), pp. 113-133.
- [2] — — *Brun's method and the Fundamental Lemma*, Proc. Sympos. Pure Math. 24 (1973), pp. 247-249.
- [3] — — *Mean value theorems for a class of arithmetic functions*, Acta Arith. 18 (1971), pp. 243-256.
- [4] — — *The distribution of polynomial sequences*, Mathematika 19 (1972), pp. 25-50.
- [5] H. L. Montgomery, *Topics in Multiplicative Number Theory*, Lecture Notes in Mathematics 227, Berlin-Heidelberg-New York 1971.
- [6] T. Nagell, *Généralisation d'un théorème de Tchebycheff*, J. de Mathématiques (8) 4 (1921), pp. 343-356.