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

THE FUNDAMENTAL LEMMA OF BRUN'S SIEVE IN A NEW SETTING

A. SCHINZEL

This paper has emerged from the need experienced in [5] to estimate from above the number of lattice points in a four dimensional cube that remain after a sieving process. A new variant of Brun's upper sieve has been devised for this purpose, however, as was pointed out to the author by Dr M. Ram Murty the same upper bound could be obtained by the large sieve and this approach has been finally adopted in [5]. Pursuing further the small sieve approach one obtains a new variant of the fundamental lemma of Halberstam and Richert embodied in the following theorem.

THEOREM 1. *Let $\mathscr{A}$ be a finite set and $\{\mathscr{T}_p\}$ a family of sets indexed by primes from a certain set $\mathscr{P}$. Assume that for a certain multiplicative function $\omega(d)$ defined on all squarefree positive integers d and suitable real numbers $X > 0$, $A_1 \geqq 1$, $A_2 \geqq 1$, A_3, $k \geqq 1$, κ we have*

$$(1) \qquad 0 \leqq \frac{\omega(p)}{p} \leqq 1 - \frac{1}{A_1} \textit{ for all primes } p,$$

$$(2) \qquad \sum_{w \leqq p < z} \frac{\omega(p)\log p}{p} \leqq \kappa \log \frac{z}{w} + A_2 \textit{ for all } w, z \textit{ with } 2 \leqq w < z,$$

$$(3) \qquad \Big|\Big|\mathscr{A} \cap \bigcap_{\substack{p \in \mathscr{P} \\ p \mid d}} \mathscr{T}_p\Big| - \frac{\omega(d)}{d} X\Big| \leqq A_3 X^{1-(1/k)} d^{k-1} \omega(d).$$

Then for all $z \leqq X$ the number

$$S(\mathscr{A}; \mathscr{P}, z) = \Big|\mathscr{A} \setminus \bigcup_{\substack{p \in \mathscr{P} \\ p < z}} \mathscr{T}_p\Big|$$

satisfies the relation

Received by the editors January 10,1984 and in revised form January 31, 1984 .

$$S(\mathscr{A};\mathscr{P},z) = X\prod_{p<z}\left(1-\frac{\omega(p)}{p}\right)$$

$$\times\left\{1+O\left(\exp-\left(\frac{u}{k^2}(\log u-\log\log 3u-\log\kappa\ -2)\right)\right.\right. \tag{4}$$

$$\left.\left.+\ O(\exp(-k(\log X)^{1/2})\right)\right\}$$

where

$$u = \frac{\log X}{\log z} \tag{5}$$

and the constants in the O symbol depend only on A_1, A_2, A_3, k *and* κ.

Theorem 1 contains as a special case theorem 2.5 of the book [**2**] of Halberstam and Richert, which is slightly obscured by the fact that they consider a sequence $\mathscr{A}$ rather than a set and define $S(\mathscr{A};\mathscr{P},z)$ accordingly. In order to obtain their result one has to take for our $\mathscr{A}$ the set of subscripts of all elements of their $\mathscr{A}$ and for $\mathscr{T}_p$ the set of subscripts of all elements divisible by p. Our theorem will not become more general if sets are replaces by sequences.

In the case $k = \kappa = 1$ the error term in the formula (4) can be improved to

$$O(\exp(-u(\log u + \log\log 3u + O(1))) + O(\exp\ -\ (\log x)^{1/2})$$

by using Rosser's sieve (see Iwaniec [**3**], p. 29). According to Prof. Iwaniec a similar improvement probably can be made in the general case (cf. Iwaniec [**4**], p.177).

COROLLARY. *For any* $\theta > 0$ *under the assumption of Theorem* 1

$$S(\mathscr{A};\mathscr{P},z) < BX\prod_{p<z}\left(1-\frac{\omega(p)}{p}\right)$$

provided $z \leqq X^{\theta}$ *and* $B = B(\theta, A_1, A_2, A_3, k, \kappa)$

This corollary inserted at the suggestion of the referee generalizes Theorem 2.2 of [**2**]. However in the most interesting case, where $\mathscr{A} \subset Z^k$, $\mathscr{T}_p \subset Z^k$ and each $\mathscr{T}_p$ is a union of residue classes mod p, the Corollary follows from the large sieve result of Gallagher [**1**] and from Lemma 4.1 of [**2**].

As an application of Theorem 1 which cannot be obtained from the quoted Theorem 2.5 we give the following

THEOREM 2. *Let* $F_1(x_1,\ldots,x_k),\ldots,F_r(x_1,\ldots,x_k)$ *be distinct irreducible polynomials with integer coefficients and let*

$$F(x_1,\ldots,x_k) = F_1(x_1,\ldots,x_k)\ldots F_r(x_1,\ldots,x_k).$$

Let $\rho(d)$ denote the number of solutions of the congruence $F(x_1, \dots, x_k) \equiv 0 \bmod d$, and assume that $\rho(p) < p^k$ for all primes p. Let c, u and x be real numbers such that $c > 0$, $u \geqq 1$ and *$x^{1/u} \geqq 2$ and let $\mathcal{Q}(x, u, c)$ be the set of all integers q having no prime divisors less thab $x^{1/u}$ and satisfying $(\log q)/(\log x) \leqq c$. Then*

$$|\{\mathbf{n} = <n_1, n_2, \dots, n_k> : 1 \leqq n_i \leqq x;\ F_i(\mathbf{n}) \in \mathcal{Q}(x, u, \deg F_i + 1) \text{ for } i = 1, 2, \dots, r| = x^k \prod_{p<x^{1/u}} \left(1 - \frac{\rho(p)}{p^k}\right)$$
$$\times \left\{1 + O_F\left(\exp\left(-\frac{u}{k^2}(\log u - \log\log 3u - \log g - 2)\right) + O_F(\exp(-k\sqrt{\log x}))\right)\right\},$$

where g is the total degree of F and the constants in the O symbol depend only on the coefficients and degrees of $F_1, \dots, F_r$.

For $k = 1$ Theorem 2 gives a slightly weaker version of Theorem 2.6 of **[2]**; log r has been replaced by log g. If one tries to apply Theorem 2.5 of **[2]** for $k > 1$ one can consider the sequence of all values $F(n_1, n_2, \dots, n_k)$ for $n_i \leqq x (1 \leqq i \leqq k)$ and the conditions Ω_1, $\Omega_2(\kappa)$ are fulfilled with $\omega(d) = \rho(d)$, $\kappa = g$ but the condition (R) is not satisfied.

Proofs of Theorems 1 and 2 follow closely the proofs of Theorems 2.5 and 2.6 of **[2]**.

PROOF OF THEOREM 1. Let

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

Following the proof of (3.14) in Chapter 2 of **[2]** we find that

$$S(\mathcal{A}; \mathcal{P}, z) = XW(z) + \theta A_3 X^{1-(1/k)} \exp(Az^{k-1}(2liz + 3));\ |\theta| \leqq 1$$
$$A = \max(\kappa, A_2) > 0$$

hence we may assume that z is large enough, i.e.

$$z \geqq B_1 = B_1(k, \kappa, A_2). \tag{6}$$

Assume first that

$$\log z \leqq (\log X)^{1/2}. \tag{7}$$

Following the proof of (3.16) in Chapter 2 of **[2]** we find that

$$S(\mathcal{A}; \mathcal{P}, z) = XW(z) \{1 + \theta(\lambda e^{1+\lambda})^{(\kappa \log\log z + c_0)/\lambda}\}$$
$$\times\ \theta' A_3 X^{1-(1/k)}\ z^{k(\kappa \log\log z + c_0)/\lambda},\ |\theta| \leqq 1,\ |\theta'| \leqq 1$$

provided

$$(8) \qquad 0 \leqq \lambda e^{1+\lambda} < 1$$

and

$$c_0 = \kappa \log\left(\frac{1}{\log 2}\right) + \frac{A_2}{\log 2}\left\{1 + A_1\left(\kappa + \frac{A_2}{\log 2}\right)\right\}.$$

If we choose

$$\frac{1}{\lambda} = \frac{1}{2k^2}\frac{\log X}{\log z(\kappa \log\log z + c_0)}$$

we have by virtue of (6) and (7)

$$S(\mathscr{A}; \mathscr{P}, z) = XW(z)\{1 + \theta \exp(-(\log x)^{1/2})\} + \theta' A_3 X^{1-(1/2k)}, |\theta| \leqq 1, |\theta'| \leqq 1$$

and (4) follows.
Assume now that

$$(9) \qquad \log z > (\log X)^{1/2}$$

and u given by (5) is large enough, that is

$$(10) \qquad u \geqq B_2 = B_2(k, \kappa, A_1, A_2).$$

Following line by line the proof of Theorem 2.1 of [2] we get for every positive integer b and every real λ satisfying (8) the inequalities

$$(11) \qquad S(\mathscr{A}; \mathscr{P}, z) \leqq XW(z)\left\{1 + 2\frac{\lambda^{2b+1}e^{2\lambda}}{1-\lambda^2 e^{2+2\lambda}}\exp\left((2b+3)\frac{c_1}{\lambda \log z}\right)\right\} + O(X^{1-(1/k)} z^{2bk+2.01k/(e^{2\lambda/\kappa}-1)})$$

$$(12) \qquad S(\mathscr{A}; \mathscr{P}, z) \geqq XW(z)\left\{1 - 2\frac{\lambda^{2b}e^{2\lambda}}{1-\lambda^2 e^{2+2\lambda}}\exp\left((2b+2)\frac{c_1}{\lambda \log z}\right)\right\} + O(X^{1-(1/k)} z^{(2b-1)k+2.01k/(e^{2\lambda/\kappa}-1)})$$

where

$$c_1 = \frac{A_2}{2}\left(1 + A_1\left(\kappa + \frac{A_2}{\log 2}\right)\right).$$

On the other hand by formula (3.5) of Chapter 2 of [2] which has been deduced from (1) and (2) only we have

$$(13) \qquad \frac{W(w)}{W(z)} = O\left(\frac{\log^\kappa z}{\log^\kappa w}\right)(2 \leqq w \leqq z)$$

and in particular

$$\frac{1}{W(z)} = O(\log^{\kappa} z). \tag{14}$$

By virtue of (10) the number

$$b = \left[\frac{u}{2k^2} - \frac{u}{2\log u}\right]$$

is positive and $\lambda = (e\kappa \log u)/u$ satisfies (8).
In view of (11), (12) and (14) we get

$$\begin{aligned} S(\mathscr{A}; \mathscr{P}, z) = XW(z)\Big\{1 &+ O\Big(\exp\Big(-2b\log\frac{1}{\lambda} + 2b\frac{c_1}{\lambda \log z}\Big)\Big) \\ &+ O\Big(\exp\Big\{-\log z\Big(\frac{u}{k} - 2bk - \frac{ek\,\kappa}{2\lambda}\Big) + \kappa \log\log z\Big)\Big)\Big\} \end{aligned}$$

and the error terms are

$$\begin{aligned} &O\Big(\exp\Big\{-\Big(\frac{u}{k^2} - \frac{u}{\log u}\Big)\log\frac{u}{e\kappa \log u} + O\Big(\frac{u}{\log u}\Big)\Big\} \\ &\quad + O\Big(\exp\Big\{-\log z\frac{uk}{2\log u} + \kappa\log\log z\Big\}\Big) \\ &= O\Big(\exp\Big\{-\frac{u}{k^2}\Big((\log u - \log\log u - \log\kappa - 2\Big)\Big\} \\ &\quad + O(\exp(-k(\log X)^{1/2})) \end{aligned}$$

by virtue of (9).

It remains to consider the case $u < B_2$. By the definition of $S(\mathscr{A}; \mathscr{P}, z)$ we have since $z = X^{1/u}$

$$S(\mathscr{A}; \mathscr{P}, z) \leqq S(\mathscr{A}; \mathscr{P}, X^{1/B_2})$$

we now apply the preceding result (with $u = B_2$) to the expression on the right, and obtain

$$S(\mathscr{A}; \mathscr{P}, z) \leqq XW(X^{1/B_2})\,\{O(1) + O(\exp(-\log x)^{1/2})\}.$$

Hence by (13)

$$S(\mathscr{A}; \mathscr{P}, z) \leqq XW(z)\,\{O(1) + O(\exp(-\log x)^{1/2})\}$$

and since $S(\mathscr{A}; \mathscr{P}, z) \geqq 0$, (4) follows.

Proof of Corollary. For $z \leqq X$ the theorem applies directly. If $z > X$ we have by (13)

$$S(A; P, z) \leqq S(A; P, X) \ll XW(X) \ll XW(z)\Big(\frac{\log z}{\log X}\Big)^{\kappa} \leqq \theta^{\kappa} XW(z).$$

Proof of Theorem 2. Let $\mathscr{A}$ be the set of all lattice points $\langle n_1, \ldots, n_k\rangle$

in the cube $1 \leqq n_i \leqq x$, $\mathscr{T}_p$ the set of all lattice points $\langle n_1, \dots, n_k \rangle$ satisfying $F(n_1, \dots, n_k) \equiv 0 \bmod p$. We take in Theorem 1

$$\omega(d) = \frac{\rho(d)}{d^{k-1}}, X = x^k, z = x^{1/u}.$$

By lemma $3A$ of [**6**] $\rho(p) \leqq gp^{k-1}$, hence (1) is satisfied with $A = g + 1$ and (2) with $\kappa = g$ and $A_2 = 3g$ (cf. [**2**], Chapter 2, formula (3.2)). As to condition (3) let us observe that the number of elements of $\mathscr{A} \cap \bigcap_{p|d} \mathscr{T}_p$ in any k-dimensional cube of size d is $\rho(d)$. Hence

$$\left[\frac{x}{d}\right]^k \rho(d) \leqq |\mathscr{A} \cap \bigcap_{p|d} \mathscr{T}_p| \leqq \left(\left[\frac{x}{d}\right] + 1\right)^k \rho(d)$$

and since $X = x^k$ we have

$$||\mathscr{A} \cap \bigcap_{p|d} \mathscr{T}_p| - \frac{\omega(d)}{d} X| \leqq (2^k - 1) X^{1-(1/k)} d^{k-1} \omega(d);$$

thus the condition (3) is fulfilled with $A_3 = 2^k - 1$.

References

1. P. X. Gallagher, *The large sieve and probabilistic Galois Theory*, Proc. Symposia Pure Math. **24** (1973), pp.91–101.

2. H. Halberstam and H.-E. Richert, *Sieve methods*, Academic Press., 1974

3. H. Iwaniec, *The error term in the linear sieve*, Acta Arith. **19** (1971), pp.1–30.

4. H. Iwaniec, *Rosser's sieve*, Acta Arith. **36** (1980), pp.171–202.

5. A. Schinzel, *Reducibility of lacunary polynomials* V, Acta Arith. **43** (1984), 423–440.

6. W. M. Schmidt, *Equations over finite fields*, *An elementary approach*, Lecture Notes in Mathematics **536**, Springer Verlag, 1976.

INSTYTUT MATEMATYCZNY PAN, UL. SNIADECKICH 8, WARSZAWA, POLAND.