ACTA ARITHMETICA
XXIV (1974)

Sieving by prime powers

by

P. X. GALLAGHER (New York, N.Y.)

To Professor C. L. Siegel
on his 75th birthday

In this note we give a simple proof for a result of H. L. Montgomery on the large sieve and its generalisation by J. Johnsen to prime-power sieving moduli, and some examples.

Montgomery's result gives an upper bound for the number of positive integers $n \leqslant N$ which remain after $f(p)$ residue classes mod p have been removed, for each prime p. The bound is $(N+O(Q^2))/\mathscr{S}(Q)$, where

$$\mathscr{S}(Q) = \sum_{q\leqslant Q}' \prod_{p|q} \frac{f(p)}{p-f(p)}; \tag{1}$$

here the dash indicates that the sum is over square-free q, and Q is a parameter $\geqslant 1$, which is generally chosen a little less than $N^{1/2}$, in order to minimise the upper bound. The resulting bound is about the same as that given by Selberg's method if $f(p)$ is constant, but is smaller if $f(p) \to \infty$.

Montgomery's proof depends on two inequalities for means of exponential sums. The first is due to Bombieri and Davenport. For arbitrary complex a_n, put

$$S(a) = \sum_{n\leqslant N} a_n e(na), \qquad Z = \sum_{n\leqslant N} |a_n|^2,$$

where $e(a) = e^{2\pi i a}$. Then

$$\sum_{q\leqslant Q} \sum_{\substack{a=1\\(a,q)=1}}^{q} \left|S\left(\frac{a}{q}\right)\right|^2 \leqslant (N+O(Q^2))Z. \tag{2}$$

For a simple proof of (2), see Bombieri's paper [1].

The second inequality is due to Montgomery. Assume, for each prime p, that $a_n = 0$ if n is in any of the $f(p)$ removed residue classes mod p.

Then, for square-free q,

$$(3)\qquad \sum_{\substack{a=1\\(a,q)=1}}^{q}\left|S\left(\frac{a}{q}\right)\right|^2 \geqslant |S(0)|^2\prod_{p|q}\frac{f(p)}{p-f(p)}.$$

Simple proofs of this inequality have been found by Wirsing, Richert and Huxley ([7], pp. 26–29).

Putting $a_n = 1$ or 0 according as n remains or not, we get from (2) and (3) that $Z^2\mathscr{S}(Q)\leqslant\big(N+O(Q^2)\big)Z$, from which Montgomery's sieve bound follows.

Montgomery remarks in [6] that the sieve assumption gives no apparent control over the sum on the left of (3) unless q is square-free. However, if, instead of primes, we sieve by an arbitrary set $\mathscr{D}$ of pairwise relatively prime moduli d (for example, the set of kth powers of primes, for some k), removing $f(d)$ residue classes mod d, for each $d\in\mathscr{D}$, a similar argument leads to a similar upper bound for the number of integers $\leqslant N$ which remain, with

$$\mathscr{S}(Q) = \sum_{q\leqslant Q}{}' \prod_{d|q}\frac{f(d)}{d-f(d)},$$

where the dash now indicates that q runs over all products of distinct elements of $\mathscr{D}$. Still, the hypothesis gives no control over the other q.

In a recent paper [4], Johnsen has solved the problem of finding a suitable lower bound for the sum in (3) for non-square-free q ([1]). However, instead of sieving by primes or a more general "independent" set of moduli, he sieves first by primes, then by squares of primes, etc. He gets the following generalisation of Montgomery's sieve result:

THEOREM. *For each prime p, remove all but $g(p)$ different residue classes* mod p. *In each of the remaining residue classes* mod p, *remove all but $g(p^2)$ different residue classes* mod p^2, *etc. Then the number of positive integers $n\leqslant N$ which remain is at most $\big(N+O(Q^2)\big)/\mathscr{S}(Q)$, with*

$$(4)\qquad \mathscr{S}(Q) = \sum_{q\leqslant Q}\prod_{p^\nu\|q}\left(\frac{p^\nu}{h(p^\nu)}-\frac{p^{\nu-1}}{h(p^{\nu-1})}\right),$$

where $h(p^\nu) = g(p)g(p^2)\dots g(p^\nu)$, the number of residue classes mod p^ν *remaining at the νth stage.*

If the sieving stops at the first stage, so that $g(p^\nu) = p$ for $\nu\geqslant 2$, then the sum (4) reduces to (1), with $f(p) = p-g(p)$.

[1] In the context of the ring of polynomials in one variable over a finite field, rather than the ring of integers.

The proof of Johnsen's result reduces, as before, to the proof that

$$(5)\qquad \sum_{\substack{a=1\\(a,q)=1}}^{q}\left|S\left(\frac{a}{q}\right)\right|^2 \geqslant |S(0)|^2 J(q),$$

where $J(q)$ is the qth term in (4), provided $a_n = 0$ if n has been removed.

If (5) holds generally for a given q, then on replacing a_n by $a_n e(n\beta)$, we get

$$\sum_{\substack{a=1\\(a,q)=1}}^{q}\left|S\left(\frac{a}{q}+\beta\right)\right|^2 \geqslant |S(\beta)|^2 J(q).$$

Proceeding by induction on the number of different prime factors of q, let $s = qr$, with $q>1$, $r>1$, and $(q,r)=1$. Then

$$\sum_{\substack{c=1\\(c,s)=1}}^{s}\left|S\left(\frac{c}{s}\right)\right|^2 = \sum_{\substack{a=1\\(a,q)=1}}^{q}\ \sum_{\substack{b=1\\(b,r)=1}}^{r}\left|S\left(\frac{a}{q}+\frac{b}{r}\right)\right|^2 \geqslant \sum_{\substack{b=1\\(b,r)=1}}^{r}\left|S\left(\frac{b}{r}\right)\right|^2 J(q)$$
$$\geqslant |S(0)|^2 J(q)J(r) = |S(0)|^2 J(s).$$

Thus it suffices to prove (5) for prime-powers. We have

$$(6)\qquad \sum_{\substack{a=1\\p\nmid a}}^{p^\nu}\left|S\left(\frac{a}{p^\nu}\right)\right|^2 = p^\nu\sum_{c=1}^{p^\nu}|S(c,p^\nu)|^2 - p^{\nu-1}\sum_{d=1}^{p^{\nu-1}}|S(d,p^{\nu-1})|^2,$$

with $S(c,q) = \sum_{n\equiv c(q)} a_n$. For each d,

$$S(d,p^{\nu-1}) = \sum_{\substack{c=1\\c\equiv d(p^{\nu-1})}}^{p^\nu} S(c,p^\nu),$$

so, by the Schwarz inequality,

$$(7)\qquad |S(d,p^{\nu-1})|^2 \leqslant g(p^\nu)\sum_{\substack{c=1\\c\equiv d(p^{\nu-1})}}^{p^\nu}|S(c,p^\nu)|^2,$$

since, by the hypothesis, there are at most $g(p^\nu)$ nonzero terms in the sum. Similarly,

$$(8)\qquad |S(0)|^2 \leqslant h(p^\nu)\sum_{c=1}^{p^\nu}|S(c,p^\nu)|^2.$$

Combining (6), (7) and (8), the left side of (6) is

$$\geqslant \big(p^\nu - p^{\nu-1}g(p^\nu)\big)\sum_{c=1}^{p}|S(c,p^\nu)|^2 \geqslant \frac{p^\nu - p^{\nu-1}g(p^\nu)}{h(p^\nu)}|S(0)|^2 = J(p^\nu)|S(0)|^2.$$

This completes the proof of (5).

Example 1. *The number of $n \leqslant N$ in whose p-adic expansion $n = a_0 + a_1 p + a_2 p^2 + \dots$ (with $0 \leqslant a_\nu < p$) no $a_\nu = 0$ occurs for $\nu < k$, for any prime p, is* (²)

$$(9) \qquad \lesssim 2^k (k!)^2 \frac{N}{\log^k N} \qquad (N \to \infty).$$

Example 2. *By comparison, for the number of $n \leqslant N$ which remain after all but an arbitrary set of $(p-1)^k$ different residue classes* mod p^k *have been removed, for each prime p, we can only get the (larger) upper bound*

$$(10) \qquad \lesssim (2k)^k k! \frac{N}{\log^k N} \qquad (N \to \infty).$$

In the first example, $g(p^\nu) = p-1$ or p according as $1 \leqslant \nu \leqslant k$ or $\nu > k$. Thus the sum (4) is in this case $\sum_{q \leqslant Q} J^{(k)}(q)$, where $J^{(k)}$ is the multiplicative function for which

$$(11) \qquad J^{(k)}(p^\nu) = J_\nu(p) = \begin{cases} \dfrac{p^{\nu-1}}{(p-1)^\nu}, & 1 \leqslant \nu \leqslant k; \\ 0, & \nu > k. \end{cases}$$

To permit an induction on k, we estimate more generally

$$\mathcal{S}_D^{(k)}(x) = \sum_{\substack{q \leqslant Q \\ (q, D)=1}} J^{(k)}(q).$$

The case $k = 1$ is in [5]. A similar sum is estimated asymptotically in [8].

Lemma. *For $x \geqslant 1$, we have*

$$(12) \qquad \mathcal{S}_D^{(k)}(x) \geqslant (k!)^{-2} \left(\frac{\varphi(D)}{D} \log x \right)^k.$$

Proof. We have [5]

$$\mathcal{S}_D^{(1)}(x) = \sum_{\substack{q \leqslant x \\ (q, D)=1}} \frac{\mu^2(q)}{\varphi(q)} \geqslant \frac{\varphi(D)}{D} \log x.$$

For $k \geqslant 2$, we put $q = q_1 q_2^2 q_3^3 \dots$, with $q_1 q_2 q_3 \dots$ square-free, and get

$$\mathcal{S}_D^{(k)}(x) = \sum J_1(q_1) J_2(q_2) \dots J_k(q_k)$$

where the sum is over $q_1 q_2^2 \dots q_k^k \leqslant x$, and $q_1 q_2 \dots q_k$ square-free and relatively prime to D, and the J_ν are the multiplicative functions defined on square-free integers by (11). Hence

(²) The notation $F \lesssim G$ stands for $\overline{\lim}\, F/G \leqslant 1$.

$$\mathcal{S}_D^{(k)}(x) = \sum_{\substack{r \leqslant x^{1/k} \\ (r, D)=1}} J_k(r) \mathcal{S}_{Dr}^{(k-1)}(x/r^k)$$

$$\geqslant (k-1)!^{-2} \sum_{\substack{r \leqslant x^{1/k} \\ (r, D)=1}} J_k(r) \left\{ \frac{\varphi(Dr)}{Dr} \log(x/r^k) \right\}^{k-1}$$

$$= (k-1)!^{-2} \left(\frac{\varphi(D)}{D} \right)^{k-1} \sum_{\substack{r \leqslant x^{1/k} \\ (r, D)=1}} J_1(r) \log^{k-1}(x/r^k).$$

The last sum is

$$\int_0^{x^{1/k}} \{\log^{k-1}(x/y^k)\}\, d\mathcal{S}_D^{(1)}(y) = -\int_0^{x^{1/k}} \mathcal{S}_D^{(1)}(y)\, d\{\dots\}$$

$$\geqslant -\int_1^{x^{1/k}} \frac{\varphi(D)}{D} \log y\, d\{\dots\} = \frac{\varphi(D)}{D} \int_1^{x^{1/k}} \log^{k-1}(x/y^k)\, d\log y.$$

Here we have used the case $k = 1$ and the fact that $\{\dots\}$ is a decreasing function of y over the last interval of integration. Putting $u = x/y^k$, we have $d\log u = -k\, d\log y$, so the last integral is

$$\frac{1}{k} \int_1^x \log^{k-1} u \cdot d\log u = \frac{\log^k x}{k^2},$$

from which (12) follows. The bound (9) follows from the case $D = 1$ on putting $Q = N^{1/2}/\log N$.

In the second example, we are sieving by the set of kth powers of primes, and

$$\mathcal{S}(Q) = \sum_{q^k \leqslant Q}' \prod_{p \mid q} \frac{p^k - (p-1)^k}{(p-1)^k},$$

where the dash indicates that the sum is over square-free q. It follows from a more general asymptotic formula of Halberstam and Richert [3] that

$$\sum_{q \leqslant x}' \prod_{p \mid q} \frac{p^k - (p-1)^k}{(p-1)^k} \sim \frac{1}{k!} \log^k x,$$

and the bound (10) follows from this on putting $x = Q^{1/k}$ and $Q = N^{1/2}/\log N$.

EXAMPLE 3. *The number of primes $a \leqslant N$ for which $a^{p-1} \equiv 1 \bmod p^2$ for no odd prime $p \leqslant N^{1/4}$ is*

$$\lesssim 32 \frac{N}{\log^2 N}.$$

Proof. The primes $a \leqslant N^{1/2}$ are negligible, so we may first remove the zero class mod p for each prime $p \leqslant N^{1/2}$; then, in each of the remaining residue class mod p, remove the unique residue class mod p^2 of multiplicative order dividing $p-1$, for each odd prime $p \leqslant N^{1/4}$. Here $g(p) = p-1$ for $p \leqslant N^{1/2}$ and $g(p^2) = p-1$ for odd $p \leqslant N^{1/2}$. As in Example 1, for $Q \leqslant N^{1/2}$,

$$\mathscr{S}(Q) = \sum_{\text{odd } r \leqslant Q^{1/2}} \frac{\mu^2(r) r}{\varphi^2(r)} \sum_{\substack{s \leqslant Q/r^2 \\ (s,r)=1}} \frac{\mu^2(s)}{\varphi(s)} \geqslant \sum_{\text{odd } r \leqslant Q^{1/2}} \frac{\mu^2(r)}{\varphi(r)} \log(Q/r^2)$$

$$\geqslant \tfrac{1}{2} \int_1^{Q^{1/2}} \log(Q/y^2)\, d\log y = \tfrac{1}{8}\log^2 Q.$$

Choosing $Q = N^{1/2}/\log N$, the result follows.

The same result (also with the constant 32) may also be obtained by combining Selberg's sieve mod p^2 with Bombieri's mean value theorem.

EXAMPLE 4. *The number of integers $a \leqslant N$ for which $a^{p-1} \equiv 1 \bmod p^2$ for no odd primes $p \leqslant N^{1/4}$ is*

$$\lesssim 8 \prod_{\text{odd } p} \left(1 + \frac{1}{p(p-1)}\right) \frac{N}{\log N}.$$

Proof. In this example, we remove $p-1$ residue classes mod p^2 for each odd prime $p \leqslant N^{1/4}$, so for $Q \leqslant N^{1/2}$,

$$\mathscr{S}(Q) = \sum_{\text{odd } q \leqslant Q^{1/2}} \mu^2(q) \prod_{p \mid q} \frac{p-1}{p^2-p+1}.$$

By the result of Halberstam and Richert mentioned earlier,

$$\mathscr{S}(Q) \sim e^{-\gamma} \prod_{\text{odd } p \leqslant Q^{1/2}} \left(1 - \frac{p-1}{p^2}\right)^{-1}$$

$$= e^{-\gamma} \prod_{\text{odd } p \leqslant Q^{1/2}} \left(1 - \frac{1}{p}\right)^{-1} \prod_{\text{odd } p \leqslant Q^{1/2}} \left(1 + \frac{1}{p(p-1)}\right)^{-1}$$

$$\sim \frac{1}{4} \log Q \prod_{\text{odd } p} \left(1 + \frac{1}{p(p-1)}\right)^{-1}.$$

Putting $Q = N^{1/2}/\log N$, the result follows.

For the analogous problems mod p^3, the sieve of Eratosthenes (combined with the prime number theorem for arithmetic progressions) leads easily to asymptotic formulae: The number of integers (primes) $a \leqslant N$ for which $a^{p-1} \equiv 1 \bmod p^3$ for no odd prime $p \leqslant N^{1/3}$ is

$$\sim N \prod_{\text{odd } p} \left(1 - \frac{p-1}{p^3}\right) \quad \left(\sim \frac{N}{\log N} \prod_{\text{odd } p} \left(1 - \frac{1}{p^2}\right)\right).$$

Numerical data for $a \leqslant 100$ and $p \leqslant 2^{25}$ is given in [2].

References

[1] E. Bombieri, *A note on the large sieve*, Acta Arith. 18 (1971), pp. 401–404.

[2] J. Brillhart, J. Tonascia, and P. Weinberger, *On the Fermat quotient*, *Computers in number theory*, Proc. Atlas Sympos. 2, Oxford 1969 (1972), pp. 213–222.

[3] H. Halberstam and H.-E. Richert, *Mean values for a class of arithmetic functions*, Acta Arith. 18 (1971), pp. 243–256.

[4] J. Johnsen, *On the large sieve method in* GF(q, x), Mathematika 18 (1971), pp. 172–184.

[5] J. H. van Lint and H.-E. Richert, *On primes in arithmetic progressions*, Acta Arith. 11 (1965), pp. 209–216.

[6] H. L. Montgomery, *A note on the large sieve*, J. London Math. Soc. 43 (1968), pp. 93–98.

[7] — *Topics in Multiplicative Number Theory*, Berlin 1971.

[8] J. W. Porter, *The generalised Titchmarsh–Linnik divisor problem*, Proc. London Math. Soc. 24 (1972), pp. 15–26.

MATHEMATICS DEPARTMENT
COLUMBIA UNIVERSITY
New York, N.Y. 10027

Received on 20. 1. 1973 (367)