References

[1] Н. И. Фельдман, *Аппроксимация некоторых трансцендентных чисел, I. Аппроксимация логарифмов алгебраических чисел*, ИАН, сер. матем., 15 (1951), pp. 53–74.
[2] — *К вопросу о мере трансцендентности числа e*, УМН 18 (1963), pp. 207–213.
[3] R. Güting, Michigan Math. J. 8 (1961), pp. 149–159.
[4] J. F. Koksma, Mh. Math. Physik 48 (1939), pp. 176–189.
[5] Th. Schneider, *Einführung in die transzendenten Zahlen*, Berlin 1955.
[6] E. Wirsing, J. Reine Angew. Math. 206 (1961), pp. 66–77.

OHIO STATE UNIVERSITY
Columbus, Ohio

Received on 9. 10. 1969

ACTA ARITHMETICA
XVIII (1971)

A larger sieve

by

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

1. Linnik's 'large sieve' gives an upper bound for the number of integers which remain in an interval of length N after $f(p)$ different residue classes (mod p) have been removed, for each prime p. In its refined form, due to Bombieri and Davenport [1], [2], and Montgomery [4], the upper bound is

$$\frac{N+CQ^2}{S(Q)}, \quad \text{where } S(Q) = \sum_{q\leqslant Q}\mu^2(q)\prod_{p|q}\frac{f(p)}{p-f(p)}, \tag{1}$$

and C is a positive constant. In the applications, Q is chosen a little less than $N^{1/2}$ to minimise the bound.

In some cases, the bound obtained is nearly best possible. For example, if the quadratic nonresidues (mod p) are removed for each prime p, the perfect squares remain. Here $f(p) = \frac{1}{2}(p-1)$ for odd p, so $S(Q) \gg Q$. Thus the upper bound is $\ll N^{1/2}$ for $Q = N^{1/2}$.

In this note we give a simple sieve method which gives a comparable bound in this example and is more effective than the large sieve when $f(p)$ is close to p. We put $g(p) = p-f(p)$ and consider also prime power moduli.

Theorem 1. *If all but $g(q)$ residue classes* (mod q) *are removed for each prime power q in a finite set $\mathscr{S}$, then the number of integers which remain in any interval of length N is at most*

$$\Big(\sum_{q\in\mathscr{S}}\Lambda(q)-\log N\Big)\Big/\Big(\sum_{q\in\mathscr{S}}\frac{\Lambda(q)}{g(q)}-\log N\Big) \tag{2}$$

provided the denominator is positive. Here $\Lambda(q) = \log p$ for $q = p^a$.

Proof. Assume Z integers n remain in a given interval of length N, and of these $Z(h, q)$ satisfy $n\equiv h$ (mod q). Then

$$Z^2 = \Big(\sum_{h=1}^{q}Z(h,q)\Big)^2 \leqslant g(q)\sum_{h=1}^{q}\big(Z(h,q)\big)^2$$

for $q\in\mathcal{S}$, since $Z(h,q)=0$ for all but $g(q)$ values of h. Summing over $\mathcal{S}$, we get

$$Z^2\sum_{q\in\mathcal{S}}\frac{\Lambda(q)}{g(q)}\leqslant\sum_{q\in\mathcal{S}}\Lambda(g)\sum_{m\equiv n(q)}1=\sum_{|d|\leqslant N}\Big(\sum_{m-n=d}1\Big)\Big(\sum_{q|d,\,q\in\mathcal{S}}\Lambda(q)\Big)$$
$$\leqslant Z\sum_{q\in\mathcal{S}}\Lambda(q)+(Z^2-Z)\log N,$$

since $\sum_{q|d}\Lambda(q)=\log|d|$, for $d\neq 0$. It follows that the expression (2) is an upper bound for Z, if the denominator is positive.

In the example above, $g(p)=\frac{1}{2}(p+1)$ for odd p, so

$$\sum_{p\leqslant Q}\frac{\log p}{g(p)}=2\log Q+O(1),\qquad \sum_{p\leqslant Q}\log p\ll Q$$

by well-known estimates. Choosing $Q=CN^{1/2}$, the bound given by (2) is $\ll N^{1/2}$ as before, for sufficiently large C.

COROLLARY. *If all but at most G residue classes* (mod q) *are removed for each $q\in\mathcal{S}$, then the number of integers which remain in any interval of length N is*

(3) $$\leqslant G,\qquad \textit{if}\quad \sum_{q\in\mathcal{S}}\Lambda(q)>G^2\log N,$$

(4) $$\leqslant 2G-1,\qquad \textit{if}\quad \sum_{q\in\mathcal{S}}\Lambda(q)\geqslant 2G\log N.$$

Proof. With an obvious notation, the theorem gives

$$Z\leqslant\frac{L-l}{L/G-l}=G+\frac{G^2l-Gl}{L-Gl}\qquad (L>Gl).$$

If $L>G^2l$, then $Z<G+1$. We may assume G is an integer, so this implies $Z\leqslant G$. If $L\geqslant 2Gl$, we get $Z\leqslant 2G-1$.

The upper bound given in (3) is certainly best possible since any G different integers will represent $\leqslant G$ different residue classes (mod q), for every q. The condition $L>G^2l$ in (3) is also best possible, if $G=1$. For example, if N is a square-free positive integer and $\mathcal{S}$ is the set of prime divisors of N, then $L=l$, while the two integers 0 and N represent only the zero class (mod p) for each $p\in\mathcal{S}$.

If $f(p)=p-G$ for $p>G$ and $f(p)=0$ for $p\leqslant G$, the bound given by (1) is $\gg\min(G\log N,G^2)$. In fact,

$$S(Q)\leqslant\sum_{q\leqslant Q}\mu^2(q)\prod_{p|q}\frac{p}{G}\ll\frac{Q^2}{G\log Q}+\frac{Q^2}{G^2}$$

so

$$\frac{N+CQ^2}{S(Q)}\gg\Big(\frac{N}{Q^2}+1\Big)\min(G\log Q,G^2),$$

from which our assertion follows, on considering separately the cases $Q^2\leqslant N^{1/2}$ and $Q^2\geqslant N^{1/2}$.

2. In [3] it was shown that the number of integers $n\leqslant N$ for which $\exp_p(n)\leqslant N^\theta$ (¹) for all primes $p\leqslant N^{1/2}$ is $\ll N^\theta\log N$, uniformly for $\theta\leqslant\frac{1}{2}-\varepsilon$, for each $\varepsilon>0$. The following result improves this.

THEOREM 2. *The number of integers $n\leqslant N$ for which $\exp_p(n)\leqslant N^\theta$ for all primes $p\leqslant N^{\theta+\varepsilon}$ is $\ll N^\theta$, uniformly for $0\leqslant\theta\leqslant 1$.*

Proof. For each prime $p\leqslant g$, we remove all residue classes (mod p) except the zero class and the classes of exponent $\leqslant x$. Since there are $\varphi(f)$ classes of exponent f for $f|p-1$ we have

(5) $$g(p)=1+\sum_{\substack{f\leqslant x\\ f|p-1}}\varphi(f).$$

The Schwarz inequality and the prime number theorem give

(6) $$\Big(\sum_{p\leqslant y}\frac{\log p}{g(p)}\Big)\Big(\sum_{p\leqslant y}g(p)\log p\Big)\geqslant\Big(\sum_{p\leqslant y}\log p\Big)^2\gg y^2.$$

From (5) we get

(7) $$\sum_{p\leqslant y}g(p)\log p\ll y+\log y\sum_{f\leqslant x}\varphi(f)\pi(y,f,1).$$

The Brun Titchmarsh theorem [1] gives the bound

$$\pi(y,f,1)\ll\frac{y}{\varphi(f)\log y},\qquad y\geqslant f^{1+\varepsilon}.$$

Hence for $y\geqslant x^{1+\varepsilon}$, the right side of (7) is $\ll xy$, and therefore, by (6),

$$\sum_{p\leqslant y}\frac{\log p}{g(p)}\gg\frac{y}{x}.$$

Put $x=N^\theta$ and $y=N^{\theta+\varepsilon}$. Theorem 1 gives a bound

$$\ll N^{\theta+\varepsilon}/(CN^\varepsilon-\log N)\ll N^\theta,$$

provided $N\geqslant N_\varepsilon$. For bounded N, the result is trivial.

(¹) We denote by $\exp_q(n)$ the least positive integer g such that $n^g\equiv 1$ (mod q) if $(n,q)=1$; otherwise, we set $\exp_q(n)=0$.

3. Schinzel has proved in [5] that if a, b are positive integers, and $b \equiv a^{\nu(p)} (\operatorname{mod} p)$ for each prime p, then $b = a^{\nu}$. In this section we show how a weaker result can be proved using the corollary to Theorem 1.

THEOREM 3. *Let a, b be positive integers and let P be a finite set of primes. Assume $b \equiv a^{\nu(q)} (\operatorname{mod} q)$ for each prime power $q = p^a$ with $p \notin P^{\nu}$. Then $b = a^{\nu}$.*

We may suppose $a > 1$, and that P contains the prime divisors of a.

LEMMA. *Let $\mathscr{S} = \mathscr{S}(k, G)$ be the set of prime powers $q = p^a$ with $p \notin P$ for which $k | \exp_q(a)$ and $\exp_q(a) \leqslant G$. Then (for fixed a, k, P),*

$$\sum_{q \in \mathscr{S}} \Lambda(q) \gg G^2 \qquad (G \geqslant G_0). \tag{8}$$

In particular, there is a $q = p^a$ with $p \notin P$ for which $k | \exp_q(a)$.

Proof. Put $e(q) = \exp_q(a)$. We first show

$$\sum_{e(q) = g} \Lambda(q) \sim \varphi(g) \log a \qquad (g \to \infty). \tag{9}$$

By the Möbius inversion formula, the sum is

$$\sum_{d|g} \mu(d) \sum_{e(q)|g/d} \Lambda(q).$$

Since $e(q)|f$ if and only if $a^f \equiv 1 \operatorname{mod} q$, the inner sum is $\log(a^{g/d} - 1)$, so the sum is

$$\sum_{d|g} \mu(d) \log(a^{g/d} - 1) = g \log a \sum_{d|g} \mu(d)/d + O\Big(\sum_{d|g} a^{-g/d}\Big),$$

from which (9) follows.

Apart from the restriction $p \notin P$, (8) follows from (9) and the fact that (for fixed k)

$$\sum_{g \leqslant G, k|g} \varphi(g) \gg G^2 \qquad (G \geqslant G_0).$$

From $a^{e(q)} \equiv 1 \operatorname{mod} q$, we get $a^{e(q)} > q$. Hence if $e(q^a) \leqslant G$, then $a \ll G$ (for fixed a and p). Thus the contribution to $\sum_{e(q) \leqslant G} \Lambda(q)$ of the powers of the primes in P is $\ll G$, and we get (8), with a different G_0.

Proof of Theorem 3. We remove all integers $n \leqslant N$ except those for which $n \equiv a^{\nu(q,n)} (\operatorname{mod} q)$ for each $q = p^a$ with $p \notin P$ and $\exp_q(a) \leqslant G$. Here $g(q) = \exp_q(a)$. By the corollary to Theorem 1 and the lemma, with $k = 1$, the number of integers $n \leqslant N$ which remain is $\ll G$ provided $G^2 \geqslant CG \log N$. Choosing $G = C \log N$, we get that $\ll \log N$ integers remain.

If b satisfies the hypothesis of the theorem, so do each of the integers $a^{\nu} b^k$. Since there are formally $\gg \log^2 N$ such integers $\leqslant N$, a contradiction with the previous paragraph is avoided only if they are not all distinct, from which we get $b^k = a^{\nu}$ for some integers k, ν with $k \neq 0$.

We may assume $(k, \nu) = 1$. Then $a = c^k$, $b = c^{\nu}$ for some integer $c > 1$. The hypothesis now reads

$$\nu \equiv k\nu(q) \operatorname{mod} \exp_q(c)$$

for each $q = p^a$, $p \notin P$. Applying the second statement of the lemma to c, k, P, we get $k|\nu$. Since $(k, \nu) = 1$, this means $k = 1$, and hence $b = a^{\nu}$.

References

[1] E. Bombieri and H. Davenport, *On the large sieve method*, Abhandlungen aus Zahlentheorie und Analysis zur Erinnerung an Edmund Landau, Berlin 1968.

[2] — — *Some inequalities concerning trigonometrical polynomials*, Ann. Scuola Norm. Sup. Pisa 23 (1969), pp. 223–241.

[3] P. X. Gallagher, *The large sieve*, Mathematika 14 (1967), pp. 14–20.

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

[5] A. Schinzel, *On the congruence $a^x \equiv b \pmod p$*, Bull. Acad. Polon. Sci. 8 (1960), pp. 307–309.

BARNARD COLLEGE, COLUMBIA UNIVERSITY
New York, N. Y.
UNIVERSITY of NOTTINGHAM
Nottingham, England

Received on 14. 10. 1969