ACTA ARITHMETICA
XIII (1967)

A problem of Erdös concerning power residue sums

by

P. D. T. A. Elliott (Nottingham)

Let k be a positive integer. Let p be a positive rational prime. If p satisfies $p \equiv 1 (\bmod k)$, we define $n_k(p)$ to be the least positive residue which is not a k-th power $(\bmod p)$. For other primes we define $n_k(p)$ to be zero.

Some years ago, in answer to a question of Mirsky, Erdös [5] proved that

$$\sum_{p<x} n_2(p) \sim c \frac{x}{\log x} \tag{1}$$

as $x \to \infty$, for a certain constant c. Moreover, he conjectured that a result of this type held for any k.

It is the purpose of the present note to prove that this expectation is justified.

THEOREM 1. *For each integer $k > 0$, and constant a which satisfies $a < 4e^{1-1/k}$, we have as $x \to \infty$, the asymptotic relation*

$$\sum_{p<x} \big(n_k(p)\big)^a \sim C_{k,a} \frac{x}{\log x},$$

where $C_{k,a}$ is a constant. In particular, if k is an odd prime, we can express $C_{k,a}$ by

$$C_{k,a} = \sum_{r=1}^{\infty} k^{-r} q_r^a.$$

In this sum q_r runs over all the rational primes.

The author would like to record his thanks to Professor Heilbronn and Dr. Cassels for their helpful advice. We note that this result has also been stated by Barban ([1], pp. 61, 62) without proof.

The proof of the theorem falls naturally into three parts. We need various lemmas. Before stating the first of these, we recall that two fields E, F are said to be *linearly disjoint* over a common subfield G, when any finite set of elements of E which are linearly independent over G remain so over F. It is well known (Zariski and Samuel [13], § 15, pp. 109), that this condition is symmetric in E and F. We now prove a result, which though of a type well-known in algebraic geometry, seems not to be readily available in the literature.

LEMMA 1. *Let E, F be two extensions of a field G, one of which is finite and normal. Then E and F are linearly disjoint over G if and only if their common subfield is G.*

Proof. We can assume, without loss of generality, that E is a finite normal extension of G, of degree n.

Suppose first that E and F are not linearly disjoint over G. Then we can find elements a_i, $i = 1, \ldots, m$, of E, which are linearly independent over G, but linearly dependent over F. Thus there are elements λ_i, $i = 1, \ldots, m$, of F, not all zero, so that

$$\sum_{i=1}^{m} \lambda_i a_i = 0. \tag{2}$$

Let θ be an element generating E over G. Then for each value of i satisfying $1 \leqslant i \leqslant m$, we can find members c_{ij} in G, so that

$$a_i = \sum_{j=0}^{n-1} c_{ij} \theta^j. \tag{3}$$

Clearly these two relations imply that

$$\sum_{j=0}^{n-1} \theta^j \sum_{i=1}^{m} c_{ij} \lambda_i = 0. \tag{4}$$

Now not all of the coefficients of the powers of θ in this equality are zero. For otherwise, the linear equations

$$\sum_{i=1}^{m} c_{ij} x_i = 0, \quad j = 0, 1, \ldots, n-1,$$

in the variables x_i, $i = 1, \ldots, m$, have a non-trivial solution in G. Such a solution would imply, by (3) and (4) that $a_1, \ldots, a_m$, were linearly dependent over G, contrary to assumption. Thus we see that θ is the root of an irreducible polynomial $f(x)$, defined over F, and of degree at most $n-1$.

Let $g(x)$ be an irreducible polynomial defining θ over G. Since E is a normal extension, $g(x)$ splits completely in E into factors $x - \beta_i$, $i = 1, \ldots, n$, say. The result which we have just proved shows that $f(x)$ divides $g(x)$ in $F(x)$, so that we can assume, without loss of generality, that

$$f(x) = \prod_{i=1}^{s} (x - \beta_i), \quad 1 \leqslant s \leqslant n-1.$$

Consider now the elementary symmetric functions of the β_i, $i = 1, \ldots, s$. These cannot all lie in G. For otherwise $f(x)$ would be defined over G, and so $g(x)$ would be reducible over G, contrary to assumption. Let σ be a symmetric function of these β_i, which does not lie in G. Then clearly σ lies in both E and F, so that

$$G \subset G(\sigma) \subseteq E \cap F.$$

This proves one half of the lemma. This result is all we shall need, but for completeness we give a short proof of the remaining half of the lemma.

Suppose now, therefore, that E and F are linearly disjoint over G, but that we can find an element a, lying in E and F, but not in G. Then $1, a$ are linearly independent over G, but not over F. This contradicts our initial hypothesis.

Hence the lemma is proved.

In what follows we shall use Q to denote the field of rational numbers.

LEMMA 2. *Let l, k be positive rational integers. Let t be a rational number which is not a power of a rational number, and for which $-t$ is not a square of a rational number. Then $\sqrt[l]{t}$ can be contained in the cyclotomic field $Q(\sqrt[k]{1})$ only if $l = 1$ or 2. If $l = 2$ then t must also be made up from squares, and primes which divide k.*

Proof. By considering the prime factors of l it is clear that we need only consider the cases when t does not lie in Q, and l is either an odd prime or 4.

If $\sqrt[l]{t}$ and so $Q(\sqrt[l]{t})$ lies in the Abelian extension $Q(\sqrt[k]{1})$, it follows from Galois theory that $Q(\sqrt[l]{t})$ must be a normal extension of Q. In particular therefore, the polynomial $x^l - t$, which has a linear factor in that extension field, must split completely into linear factors over it, so that the element $S = \exp(2\pi i/l)$ must also be contained in the field $Q(\sqrt[l]{t})$. Thus we have the situation,

$$Q \subseteq Q(\sqrt[l]{1}) \subseteq Q(\sqrt[l]{t}).$$

Since we are assuming that l is a prime power, and t is not, then $x^l - t$ must be irreducible over Q (Zariski and Samuel [13], Chapter 2, theorem 7).

Thus the degree of $Q(\sqrt[l]{t})$ over Q is l. Since $Q(\sqrt[l]{1})$ is of degree $\varphi(l)$ over Q, we see that $\varphi(l)$ divides l, so that l must be even.

It remains therefore only to deal with the case $l = 4$. In this case it is easy to see that $\zeta = i$, and $x^4 - t$ must split into $(x^2 - \sqrt{t})(x^2 + \sqrt{t})$ over the field $Q(i)$, where each quadratic factor is irreducible over $Q(i)$. Thus, the fields $Q(i)$ and $Q(\sqrt{t})$ must coincide, and so therefore do their non-trivial automorphisms defined by $i \to -i$, and $\sqrt{t} \to -\sqrt{t}$. From what we have said there must be rational numbers a, b so that

$$i = a + b\sqrt{t}.$$

Under the automorphism $\sqrt{t} \to -\sqrt{t}$ we obtain that

$$-i = a - b\sqrt{t},$$

so that $i = b\sqrt{t}$, and $t = -b^{-2}$. This final result is contrary to hypothesis, and our lemma is therefore proved, save for the final assertion. Before proving it we note that we could have chosen a real value of $\sqrt[l]{t}$, so that $Q(\sqrt[l]{t})$ would be real and therefore could not contain the complex number ζ. We have preferred the above proof since it is in some ways more natural, and is in a form suitable for generalization.

For the proof of the final assertion we note that we may clearly assume that t is a squarefree integer. The discriminant of $Q(\sqrt{t})$ is then $4t$ if $t = 2$ or $3 \pmod 4$, and t if $t \equiv 1 \pmod 4$. The rational primes which divide this discriminant ramify in $Q(\sqrt{t})$, and so in $Q(\sqrt[k]{1})$.

LEMMA 3. *In addition to the definitions of Lemma 2 let q be odd, and let $q_1, \ldots, q_r$ be rational primes. Then the degree of the field $Q(\sqrt[k]{1}; \sqrt[l]{q_1}, \ldots, \sqrt[l]{q_r})$ over Q is $l^r\varphi(k)$.*

Proof. We consider the fields

$$K_i = Q(\sqrt[k]{1}; \sqrt[l]{q_1}, \ldots, \sqrt[l]{q_i}), \quad i = 1, \ldots, r, \quad K_0 = Q(\sqrt[k]{1}).$$

Let us suppose, for the moment, that we have shown the result for K_i, $1 \leqslant i < s$. Then the result holds for K_{i+1} unless, by Lemma 1, K_i and $Q(\sqrt[l]{q_{i+1}})$ have a common subfield which properly includes Q, L say.

It is clear from what we have said that the polynomial $x^l - q_{i+1}$ must then be reducible over L, and so in particular there are integers u, t_{i+1}, $0 < t_{i+1} < l$, so that

$$\zeta^u (\sqrt[l]{q_{i+1}})^{t_{i+1}}$$

lies in L, and, therefore, so does $(\sqrt{q_{i+1}})^{t_{i+1}}$.

But by our hypothesis we can find c_j, $j = 0, 1, \ldots, l-1$, in K_{i-1} so that

$$(5) \qquad (\sqrt[l]{q_{i+1}})^{t_{i+1}} = \sum_{j=0}^{l-1} c_j (\sqrt[l]{q_i})^j.$$

Clearly, the automorphisms of K_i which leave K_{i-1} fixed, are given by

$$\sigma_\nu\colon \sqrt[l]{q_i} \to \zeta^\nu \sqrt[l]{q_i}, \qquad \nu = 0, 1, \ldots, l-1.$$

Since the polynomial $x^l - q_{i+1}^{t_{i+1}}$ is left invariant by each of these automorphisms σ_ν, there is an integer μ, $0 \leqslant \mu < l$, so that

$$\sigma_1\{(\sqrt[l]{q_{i+1}})^{t_{i+1}}\} = \zeta^\mu (\sqrt[l]{q_{i+1}})^{t_{i+1}}.$$

Thus, by equating the two expressions for $\zeta^\mu(\sqrt[l]{q_{i+1}})^{t_{i+1}}$, we see that

$$\zeta^\mu \Big(\sum_{j=0}^{l-1} c_j (\sqrt[l]{q_i})^j\Big) = \sum_{j=0}^{l-1} c_j \zeta^j (\sqrt[l]{q_i})^j,$$

and therefore

$$(\zeta^\mu - \zeta^j) c_j = 0, \quad j = 0, 1, \ldots, l-1.$$

It is clear from this that $c_j = 0$ unless $j = \mu$, and therefore

$$(\sqrt[l]{q_{i+1}})^{t_{i+1}} = c_\mu (\sqrt[l]{q_i})^\mu.$$

It follows from this that we can find integers $t_{i+1}, t_i = \mu$, not both zero, and in absolute value less than l, so that

$$\sqrt[l]{(q_i^{t_i} q_{i+1}^{t_{i+1}})}$$

lies in K_{i-1}.

Continuing this process, we see that if the lemma does not hold, then we finally arrive at integers t_i, satisfying $0 \leqslant t_i < l$, for $i = 1, \ldots, s$, so that $t_s \neq 0$, and

$$\sqrt[l]{\Big(\prod_{i=1}^{s} q_i^{t_i}\Big)}.$$

lies in $K_0 = Q(\sqrt[k]{1})$.

Let $l = q^e$, and suppose, as we clearly may, that not all of the integers t_i are divisible by q. Our construction shows that $e \geqslant 1$ must hold, and clearly, the note which we have made shows that the product

$$\prod_{i=1}^{s} q_i^{t_i}$$

is not a qth power of a rational number. We can therefore apply our previous lemma, and we see that we must have that both l and q have the value 2. This contradicts our initial hypothesis that q is odd, and so the lemma is proved.

If l is a power of 2, then the situation is a little more complicated. Let us consider the particular case

$$L = Q(\sqrt[k]{1}) \cap Q(\sqrt[l]{q_1}).$$

If $L \neq Q$, then L is a normal extension of Q, and the polynomial $x^l - q_1$, which is irreducible over Q, splits into m conjugate irreducible polynomials over L, where $m|l$. Thus, we can find a power of 2, 2^e say, with $e \geqslant 1$, so that $q_1^{2^{-e}}$ lies in $Q(\sqrt[k]{1})$. By Lemma 2 this can only happen if $e = 1$, and q_1 is a divisor of k.

This case, if it occurs, means that the polynomial $x^l - q_1$ splits into two conjugate polynomials over L, each of degree $\frac{1}{2}l$, so that L is a quadratic extension of Q. Since L would then contain $\sqrt{q_1}$, the only possibility for $L \neq Q$, is $Q(\sqrt{q_1})$. This situation can actually occur, for it is well-known (see for example Weiss [12], 7-3-1, p. 260), that the field $Q(\sqrt[q_1]{1})$ contains the quadratic subfield

$$Q\left(\sqrt{\{(-1)^{(1/2)(q_1-1)}q_1\}}\right).$$

Thus we see that the degree of the field $Q(\sqrt[k]{1}, \sqrt[l]{q_1})$ over Q, is $l\varphi(k)$ unless $\sqrt{q_1}$ lies in $Q(\sqrt[k]{1})$, when it is $\frac{1}{2}l\varphi(k)$. In the former case, the algebraic integers

$$(\sqrt[l]{q_1})^j, \quad j = 0, 1, \ldots, n-1, \tag{6}$$

are a field basis for $Q(\sqrt[k]{1}, \sqrt[l]{q_1})$ over $Q(\sqrt[k]{1})$, with $n = l$. In the latter case we have a similar result with $n = \frac{1}{2}l$.

When considering the field

$$Q(\sqrt[k]{1}, \sqrt[l]{q_1}, \sqrt[l]{q_2})$$

we proceed as in the proof of Lemma 3, and show that either

$$Q(\sqrt[k]{1}, \sqrt[l]{q_1}) \cap Q(\sqrt[l]{q_2}) = Q,$$

or we can find integers a, b, $0 < b < 2^e$ and $e \geqslant 1$, so that $\sqrt[2^e]{(q_2^b q_1^{-a})}$ lies in $Q(\sqrt[k]{1})$. Thus, by Lemma 2, q_2 must also be a divisor of k.

Indeed, proceeding on the lines of Lemma 3, we can prove, by inducting on r, that the only possible common subfields of $Q(\sqrt[l]{q_r})$ and

$$G_{r-1} = Q(\sqrt[k]{1}; \sqrt[l]{q_1}, \ldots, \sqrt[l]{q_{r-1}})$$

are Q and $Q(\sqrt{q_r})$. Moreover, if at the rth stage this actually occurs, then a field basis for the compositum over G_{r-1} is

$$(\sqrt[l]{q_r})^j, \quad j = 0, 1, \ldots, \tfrac{1}{2}l.$$

We now differentiate between two possible cases. Firstly we consider the case when k is divisible by 4. By what we have already noted, the field $Q(\sqrt[k]{1})$ contains $Q(\sqrt[q_r]{1})$ when $q_r|k$, and this field in turn contains $\sqrt{(-1)^{(1/2)(q_r-1)}q_r}$. Moreover, the algebraic integer i is also contained in $Q(\sqrt[k]{1})$, and so therefore is $\sqrt{q_r}$. Putting these results together, we see that the degree of G_r (with an obvious definition) over Q is

$$2^{-t}l^r\varphi(k),$$

where t denotes the number of primes q_i, $i = 1, \ldots, r$, which divide k.

The second alternative which we mentioned arises when 2 divides k exactly. We can apply the arguments which we have just used, but we need a little more calculation to determine the quadratic subfields of $Q(\sqrt[k]{1})$. In the application we are interested in, we can take $l = 2$ when k is exactly divisible by 2, and we shall here limit ourselves to this case. More especially, we show that the degree over Q of

$$H_r = Q(\sqrt[k]{1}; \sqrt{q_1}, \ldots, \sqrt{q_r}), \quad r = 0, 1, 2, \ldots,$$

is $2^{-t+r}\varphi(k)$, where t now represents the number of the primes q_i, which divide k, and also satisfy $q_i \equiv 1 \pmod 4$. We give a proof by inducting on i the number of primes.

Suppose that we have proved the result for up to $r-1$ primes q_i, the case $r = 0$ being trivially true. Then if

$$H_{r-1} \cap Q(\sqrt{q_r}) = L$$

we have to show that L is $Q(\sqrt{q_r})$ if q_r divides k and satisfies $q_r \equiv 1 \pmod 4$, and is Q otherwise. Now since 2 divides k exactly, the discriminant of $Q(\sqrt[k]{1})$ is not divisible by 2 (Weiss [12], 7-5-8, p. 266). Hence 2 does not ramify in $Q(\sqrt[k]{1})$. Thus if $Q(\sqrt{q_r})$ lies in $Q(\sqrt[k]{1})$, then $q_r \equiv 1 \pmod 4$

must hold, since otherwise the discriminant of $Q(\sqrt{q_r})$ would be $4q_r$, and 2 would ramify in $Q(\sqrt[k]{1})$. Conversely, if $q_r \equiv 1 \pmod 4$ is satisfied, then $\frac{1}{2}(q_r-1)$ is even, and $Q(\sqrt[k]{1})$ contains $Q(\sqrt{q_r})$.

We now show that L is contained in $Q(\sqrt[k]{1})$, and the stated result will then be immediate. For, if L is not Q, and the polynomial x^2-q_r is irreducible over H_{r-1}, then

$$H_{r-2}(\sqrt{q_r}) \subseteq H_{r-2}(\sqrt{q_{r-1}}),$$

and these fields must coincide. By comparing their discriminants we see that we must have $q_r = q_{r-1}$, and this contradicts our initial hypotheses. Thus x^2-q_r is reducible over H_{r-2}, and

$$L = H_{r-1} \cap Q(\sqrt{q_r}) \subseteq H_{r-2} \cap Q(\sqrt{q_r}).$$

Stepping down through the primes q_i, we see that L does in fact lie in $Q(\sqrt[k]{1})$.

Summarizing our results we can state the following result.

LEMMA 4. *If l is a power of 2, then the degree of the field $Q(\sqrt[k]{1}; \sqrt[l]{q_1}, \ldots, \sqrt[l]{q_r})$ over Q is $c(k)l^r\varphi(k)$ where $c(k)$ is bounded below by a constant depending only upon k. In particular, $c(k)$ is 2^{-t} with t equal to the number of primes q_i dividing k, when $4|k$. If 2 divides k exactly and $l=2$ then we get a similar result, with a t which counts those q_i dividing k and also satisfying $q_i \equiv 1 \pmod 4$.*

LEMMA 5. *Let $l_1 l_2 \ldots l_s$ be the factorization of k into prime powers. For r distinct rational primes $q_1, \ldots, q_r$, let K_r denote the field*

$$Q(\sqrt[k]{1}; \sqrt[l_1]{q_1}, \ldots, \sqrt[l_1]{q_r}; \sqrt[l_2]{q_1}, \ldots, \sqrt[l_2]{q_r}; \ldots; \sqrt[l_s]{q_1}, \ldots, \sqrt[l_s]{q_r}),$$

and let n_r denote its degree over Q. Then we have the estimate

$$n_r = 2^{-t}k^r\varphi(k)$$

where t is zero if k is odd, and otherwise has the values in Lemma 4.

Proof. Let $K_r^{(i)}$, $i = 1, 2, \ldots, s$, denote the fields corresponding to K_r, but containing only the l_1th, l_2th, $\ldots$, l_ith roots of the q_j. If we prove at the ith stage that

$$K_r^{(i)} \cap Q(\sqrt[k]{1}; \sqrt[l_{i+1}]{q_1}, \ldots, \sqrt[l_{i+1}]{q_r}) = Q(\sqrt[k]{1}) \tag{7}$$

then the result will follow from Lemmas 1 and 4.

To prove this result we first note that the L. H. side clearly contains the R. H. side. Denoting the L. H. side by L, we see that if L contains $Q(\sqrt[k]{1})$ properly, then its degree over $Q(\sqrt[k]{1})$ divides both the degrees of $K_r^{(i)}$ and the field

$$Q(\sqrt[k]{1}; \sqrt[l_{i+1}]{q_1}, \ldots, \sqrt[l_{i+1}]{q_r})$$

over $Q(\sqrt[k]{1})$. This can only occur if l_{i+1} has a factor in common with one of the l_j, $j = 1, \ldots, i$, and by our choice of the l_j this cannot happen.

Thus the lemma is proved.

LEMMA 6. *Let E, F be normal extensions of G. Then a prime ideal splits completely in the compositum of E and F if and only if it splits completely in E and F.*

Proof. For a proof of this result we refer to Hasse [6] I Erl. 17, p. 50.

LEMMA 7. *Let E, F be algebraic number fields, and let θ in $\overline{F}$ generate F over E, with $f(x) = 0$ as its defining equation. Then with finitely many exceptions, the prime ideals $\mathfrak{p}$ of $\overline{E}$ split completely in $\overline{F}$ if and only if $f(x)$ is completely reducible when considered in the residue class ring $\overline{E}/\mathfrak{p}$.*

Proof. For a proof we refer to Weiss [12], § 4-9, p. 168.

LEMMA 8. *Let $S(x; q_1, \ldots, q_r)$ denote the number of rational primes p, not exceeding x, for which $q_1, \ldots, q_r$ are all k-th powers residues* (mod p). *Then we have the relation*

$$S(x; q_1, \ldots, q_r) = \frac{1}{n_r}\sum_{N\mathfrak{p}<x} 1 + O(x^{1/2})$$

where the prime ideals $\mathfrak{p}$ are counted in the ring of integers of K_r, as defined earlier in Lemma 5, and n_r denotes the degree of K_r over Q.

Proof. If p is a rational prime satisfying $p \equiv 1 \pmod k$, then p splits completely in the cyclotomic field $Q(\sqrt[k]{1})$ into $\varphi(k)$ conjugate prime ideals. Let a typical one of these be $\mathfrak{p}$. Then if p is counted in $S(x; q_1, \ldots, q_r)$ we can find rational integers y_j, so that

$$q_j \equiv y_j^k \pmod p, \quad j = 1, \ldots, r,$$

from which

$$q_j \equiv y_j^k \pmod{\mathfrak{p}}, \quad j = 1, \ldots, r. \tag{8}$$

Since $\mathfrak{p}$ is of degree 1, any primitive root (mod p) is also a primitive root (mod $\mathfrak{p}$) in $Q(\sqrt[k]{1})$. It follows immediately from this that, if (8) is satisfied by integers y_j of $Q(\sqrt[k]{1})$, then it is also satisfied by rational integers y_j. Moreover, q_j is a kth power $(\mathrm{mod}\, p)$ if and only if it is an lth power $(\mathrm{mod}\, p)$ for each prime-power l which divides k exactly.

Let l be an odd prime power exactly dividing k. Then $\sqrt[l]{q_1}$ generates $Q(\sqrt[k]{1}, \sqrt[l]{q_1})$ over $Q(\sqrt[k]{1})$, and is an integer of the former field. Thus, by Lemma 7, with $f(x) = x^l - q_1$, q_1 is an lth power residue $(\mathrm{mod}\, \mathfrak{p})$ if and only if $\mathfrak{p}$ splits completely in $\overline{Q(\sqrt[k]{1}, \sqrt[l]{q_1})}$, save for finitely many prime ideals $\mathfrak{p}$.

If now l is a power of two, and $\sqrt{q_1}$ does not lie in $Q(\sqrt[k]{1})$ the same proof applies. If, on the other hand, $\sqrt{q_1}$ does lie in $Q(\sqrt[k]{1})$, then a basis for $Q(\sqrt[k]{1}, \sqrt[l]{q_1})$ over $Q(\sqrt[k]{1})$ is given by

$$(\sqrt[l]{q_1})^j, \quad j = 0, 1, \ldots, \tfrac{1}{2}l - 1.$$

We now take $f(x) = x^{l/2} - \sqrt{q_1}$ in Lemma 7, and see that q_1 is an lth power $(\mathrm{mod}\, \mathfrak{p})$ if and only if $x^{l/2} - \sqrt{q_1}$ is completely reducible $(\mathrm{mod}\, \mathfrak{p})$, and this happens if and only if $\mathfrak{p}$ splits completely in $\overline{Q(\sqrt[k]{1}, \sqrt[l]{q_1})}$. Once again we must allow for finitely many exceptions for $\mathfrak{p}$.

Carrying out these operations for the primes $q_1, \ldots, q_r$, we see from Lemma 6 that $S(x; q_1, \ldots, q_r)$ counts $\varphi(k)$ times essentially all those primes $\mathfrak{p}$ of $\overline{Q(\sqrt[k]{1})}$ which satisfy $N\mathfrak{p} < x$, and which split completely in the ring $\overline{K}_r$. In other words, the rational prime ideals generated by the primes p counted in $S(x; q_1, \ldots, q_r)$ split completely in $\overline{K}_r$.

The statement of the lemma is now immediate, the error term allowing for the finitely many primes p from which exceptional prime ideals $\mathfrak{p}$ of $\overline{Q(\sqrt[k]{1})}$ may arise, and also for the fact that the sum on the R. H. S. of the equation may count ideals of degree exceeding one. For clearly the number of these does not exceed

$$n_r\Big(\sum_{p^2<x} 1 + \sum_{p^3<x} 1 + \ldots\Big) = O(x^{1/2}).$$

As it is stated the error term is of course not necessarily uniform with respect to the primes q_i, $i = 1, \ldots, r$. Such uniformity can be effected at the cost of a little complication provided we introduce some 'small' additional terms into the error term. We shall say a little more concerning this later, but do not need it for our immediate application.

LEMMA 9. *For any algebraic number field K, we have the asymptotic relation*

$$\sum_{N\mathfrak{p}<x} 1 \sim \frac{x}{\log x}$$

as $x \to \infty$.

Proof. This result is, of course, the well-known Prime-Ideal Theorem. For a detailed account we refer to Landau [8].

We can apply this result to Lemma 8, and obtain, as $x \to \infty$, the relation

$$S(x; q_1, \ldots, q_r) \sim \frac{1}{n_r} \cdot \frac{x}{\log x}. \tag{9}$$

We shall need this later in the case when k is an odd prime.

This completes what we need for the first section of the proof. For the second we need some further definitions. In what follows we shall denote the principal ideal generated by an element μ, in the appropriate ring, by $[\mu]$.

From now on until further notice we shall assume that k is an odd prime.

Let $\varrho = \exp(2\pi i/k)$, and $\lambda = 1 - \varrho$. An algebraic integer a, of the field $Q(\sqrt[k]{1})$, is said to be *primary* if $[\lambda] \nmid a$, and if we can find a rational integer w, so that

$$a \equiv w\, (\mathrm{mod}\, [\lambda^2]).$$

We now recall the definition of the Eisenstein symbol.

If $\mathfrak{p}$ is a prime ideal of $\overline{Q(\sqrt[k]{1})}$, and $\mathfrak{p} \nmid [\lambda a]$, then there is a unique rational integer v, which satisfies $0 \leqslant v < k$, and

$$a^t \equiv \varrho^v (\mathrm{mod}\, \mathfrak{p}), \qquad t = \frac{1}{k}(N\mathfrak{p} - 1).$$

We define the *Eisenstein symbol* of $a (\mathrm{mod}\, \mathfrak{p})$ to be

$$\left(\frac{a}{\mathfrak{p}}\right)_k = \varrho^v.$$

Thus, for prime ideals of first degree, when it is defined the symbol has the value 1 if and only if a is a kth power residue $(\mathrm{mod}\, \mathfrak{p})$. More generally, if $\mathfrak{b}$ is an ideal of $\overline{Q(\sqrt[k]{1})}$, and $[\lambda a]$, $\mathfrak{b}$ have no proper common ideal factors, we define

$$\left(\frac{a}{\mathfrak{b}}\right)_k = \prod_{\mathfrak{p} | \mathfrak{b}} \left(\frac{a}{\mathfrak{p}}\right)_k,$$

where the product is taken over the prime ideal divisors of $\mathfrak{b}$. We need the following result concerning this symbol.

LEMMA 10. *If $t \neq k$ is a rational prime, and a in $Q(\sqrt[k]{1})$ is primary, so that the ideals $[a]$, $[r]$ are coprime, then*

$$\left(\frac{t}{[a]}\right)_k = \left(\frac{a}{[t]}\right)_k.$$

Proof. A proof of this reciprocity law, due to Eisenstein, is given in Landau [9], Satz 1032, p. 303.

This is enough for our needs, but it is perhaps worth including the following result, as it enables us to give more complete results later on.

LEMMA 11. *Let a be an algebraic integer of $Q(\sqrt[k]{1})$, and let γ denote the trace of $(k\lambda)^{-1}(a-1)$ taken from $Q(\sqrt[k]{1})$ down to Q. Then if $a \equiv 1 (\mathrm{mod}\,[k\lambda])$, we have that*

$$\left(\frac{k}{[a]}\right)_k = \varrho^{\gamma}.$$

Proof. This result is proved by Hasse [7].

We need some more definitions.

Let K be an algebraic number field. If K is generated by the element θ, then θ may have some real conjugates θ_i, $i = 1, \ldots, d$. Let a be an integer of $\overline{K}$. Clearly, under a mapping $\theta \to \theta_i$, a is taken into a real number. If this number is positive for each value of i, we say that θ is *totally positive*, and write $a \succ 0$.

Let $\mathfrak{f}$ be an ideal of $\overline{K}$. Two ideals $\mathfrak{a}$, $\mathfrak{b}$ of $\overline{K}$ are said to be *equivalent* (mod $\mathfrak{f}$), if $(\mathfrak{a}, \mathfrak{f}) = (\mathfrak{b}, \mathfrak{f}) = [1]$, and if, furthermore, there are two integers a, β of $\overline{K}$, which satisfy the conditions,

$$[a]\mathfrak{a} = [\beta]\mathfrak{b}, \quad a \equiv \beta \equiv 1 (\mathrm{mod}\,\mathfrak{f}), \quad a \succ 0, \quad \beta \succ 0.$$

In such a case we write $\mathfrak{a} \sim \mathfrak{b} (\mathrm{mod}\,\mathfrak{f})$. As is well known, the above definition divides the ideals of $\overline{K}$ into a finite number of equivalence classes, and we shall denote this number by $h(\mathfrak{f})$.

We now need a further result concerning ideal classes, and we use the same terminology.

LEMMA 12. *The number of prime ideals $\mathfrak{p}$ of $\overline{K}$ satisfying $N\mathfrak{p} < x$, and belonging to a particular ideal class* (mod $\mathfrak{f}$), *is, as $x \to \infty$,*

$$(1+o(1))\frac{1}{h(\mathfrak{f})} \cdot \frac{x}{\log x}.$$

Proof. This result, which is not necessarily uniform with respect to $\mathfrak{f}$, is proved by Landau ([8], Satz LXXXV, p. 112). By taking $\mathfrak{f} = [1]$ we see that this lemma includes Lemma 9.

We now apply these results to give a preliminary estimation for $S(x; q_1, \ldots, q_r)$.

For the time being, let $\mathfrak{N}_r = [k\lambda q_1 \ldots q_r]$ and let no q_i be k. We first show that the set of values

$$\left(\frac{q_j}{\mathfrak{p}}\right)_k, \quad j = 1, \ldots, r,$$

when they exist, depend only upon the ideal class (mod $\mathfrak{N}_r$) to which $\mathfrak{p}$ belongs.

For, if $\mathfrak{p}_1 \sim \mathfrak{p}_2 (\mathrm{mod}\,\mathfrak{N}_r)$, we can find integers ζ, δ of $Q\sqrt[k]{1}$, so that

$$[\zeta]\mathfrak{p}_1 = [\delta]\mathfrak{p}_2, \quad \zeta \equiv \delta \equiv 1 (\mathrm{mod}\,\mathfrak{N}_r), \quad \zeta \succ 0, \quad \delta \succ 0.$$

Now the integers ζ, δ are clearly primary, and so we may apply Lemma 10 to show that for each j, $j = 1, \ldots, r$,

$$\left(\frac{q_j}{[\zeta]}\right)_k = \left(\frac{\zeta}{[q_j]}\right)_k = 1, \tag{10}$$

since $\zeta \equiv 1 (\mathrm{mod}\,[q_j])$. Similarly we can prove that for each j,

$$\left(\frac{q_j}{[\delta]}\right)_k = 1.$$

Thus, we have the relations

$$\left(\frac{q_j}{\mathfrak{p}_1}\right)_k = \left(\frac{q_j}{\mathfrak{p}_1[\zeta]}\right)_k = \left(\frac{q_j}{\mathfrak{p}_2[\delta]}\right)_k = \left(\frac{q_j}{\mathfrak{p}_2}\right)_k. \tag{11}$$

If now, one of the q_j is k, then we apply Lemma 11 in place of Lemma 10. Thus, in place of the step (10), we see that by taking $a = \zeta$ in Lemma 11, we have that γ satisfies $\gamma \equiv 0$ (mod $[k]$), and

$$\left(\frac{k}{[\zeta]}\right)_k = 1.$$

The step (11) can therefore still be made.

Hence if k is an odd prime, we have for $S(x; q_1, \ldots, q_r)$ the estimate

$$S(x; q_1, \ldots, q_r) = \frac{1}{k-1} \sum_{\mathfrak{a}} \sum_{\substack{N\mathfrak{p} < x \\ \mathfrak{p} \sim \mathfrak{a} (\mathrm{mod}\,\mathfrak{N}_r)}} 1 + R \tag{12}$$

for a certain error term R. Here $\mathfrak{a}$ runs through a set of representatives from certain ideal classes (mod $\mathfrak{N}_r$). Let us now estimate R in detail.

During the argument we assumed that the prime ideals $\mathfrak{p}$ which we were dealing with did not divide λq_i, $i = 1, \ldots, r$. Thus we can account for those $\mathfrak{p}$ which are so ruled out, by taking a term $O(r)$ in R. Moreover, in the R. H. double-sum of (12), we have possibly included prime ideals which are not of degree 1. In order to allow for these R must contain a further error of not more than

$$\frac{1}{k-1}\sum_{f=2}^{\infty}\sum_{N\mathfrak{p}=p^f<x} 1 = O(x^{1/2}).$$

Thus, we see that we may take R to be $O(r+x^{1/2})$.

We now apply Lemma 12 to (12), and obtain as $x\to\infty$, the result

$$S(x; q_1, \ldots, q_r) \sim \frac{1}{k-1}\sum_{\mathfrak{a}}\frac{1}{h(\mathfrak{N}_r)}\cdot\frac{x}{\log x}.$$

Now we have already shown in (9) that

$$S(x; q_1, \ldots, q_r) \sim \frac{1}{n_r}\cdot\frac{x}{\log x},$$

where, by Lemma 5, $n_r = (k-1)k^r$. Comparing these two estimates we see that

$$\sum_{\mathfrak{a}} 1 = k^{-r}h(\mathfrak{N}_r). \tag{13}$$

The expression (12), along with the estimate for R, and (13), is now in a form suitable for the application of a generalization of the sieve of A. Selberg. All of our estimates up until now have not been necessarily uniform with respect to the primes q_i, $i = 1, \ldots, r$. The following lemma will enable us to obtain a uniform inequality which will suffice for our purposes.

LEMMA 13. *Let $\mathfrak{f}$ be an ideal in $\bar{K}$, with $h(\mathfrak{f})$ corresponding ideal classes. Then we can find a positive constant g, depending only upon K, so that if $x \geqslant 2$, and $N\mathfrak{f} < x^g$,*

$$\sum_{\substack{N\mathfrak{p}<x\\ \mathfrak{p}\sim\mathfrak{a}(\mathrm{mod}\,\mathfrak{f})}} 1 < \frac{c_1}{h(\mathfrak{f})}\cdot\frac{x}{\log x}.$$

Proof. A proof of this result is given in Rieger [10], Satz 5, p. 161, and Satz 7, p. 164.

Returning to our consideration of $S(x; q_1, \ldots, q_r)$ when k is an odd prime, we see that if $q_1 < q_2 < \ldots < q_r < c_2\log x$, for a small but fixed constant c_2, then by a well-known estimate from elementary number theory,

$$N([k\lambda q_1 \ldots q_r]) < x^g,$$

so that by (12), (13) and Lemma 13,

$$S(x; q_1, \ldots, q_r) \leqslant \frac{1}{k-1}\sum_{\mathfrak{a}}\frac{c_2}{h(\mathfrak{N}_r)}\cdot\frac{x}{\log x} + O(x^{1/2}).$$

Thus

$$S(x; q_1, \ldots, q_r) = O\left(k^{-r}\frac{x}{\log x} + x^{1/2}\right). \tag{14}$$

This completes our considerations of what we need for the second part of the proof.

For the third and final section we need some further lemmas. In these final lemmas k need not be a prime.

LEMMA 14. *Let $1 \leqslant a_1 < a_2 < \ldots < a_Z \leqslant N$ be distinct rational integers. For any integer r, and prime p, let $Z(r; p)$ denote the number of the a_i which satisfy $a_i \equiv r(\mathrm{mod}\,p)$. Then we have the following inequality:*

$$\sum_{p\leqslant N^{1/2}} p\sum_{r=0}^{p-1}\left(Z(r; p) - \frac{Z}{p}\right)^2 \leqslant 2.2NZ.$$

Proof. For a proof of this example of Linnik's large sieve, we refer to Davenport and Halberstam [4].

LEMMA 15. *Let $\psi(x, y)$ denote the number of rational integers, not exceeding x, which are made up entirely from primes $p \leqslant y$. Then, if for a fixed δ satisfying $0 < \delta < 1$ we have that $x \geqslant y \geqslant (\log x)^{1/\delta}$, then for any $\varepsilon > 0$,*

$$\psi(x, y) > c(\delta, \varepsilon)x^{1-\delta-\varepsilon}.$$

Here $c(\delta, \varepsilon)$ is a constant depending upon δ and ε only.

Proof. This is a sharpened form of the corresponding result by Erdös in his paper, already mentioned. Suppose first that $y < x^{\varepsilon}$, and define a positive integer k by $y^k < x \leqslant y^{k+1}$. Clearly we have that

$$\psi(x, y) \geqslant \frac{1}{k!}\Big(\sum_{p\leqslant y} 1\Big)^k > y^k(2k\log y)^{-k}$$
$$> x^{1-\varepsilon}(2k\log y)^{-k} > c_1(\delta, \varepsilon)x^{1-\delta-}.$$

For if x is large enough our hypotheses guarantee that

$$(2k\log y)^k \leqslant (2\log x)^k \leqslant \exp\left(\frac{\log x}{\log y}\log(2\log x)\right) \leqslant c_4x^{\delta}.$$

If, on the contrary, $y \geqslant x^{\varepsilon}$, then let $r = [1/\varepsilon] \geqslant 1$. If x is, once again, large compared with ε, we have,

$$\psi(x, y) \geqslant \frac{1}{r!}\Big(\sum_{p \leqslant x^{\varepsilon}} 1\Big)^r > c_2(\varepsilon) x^{\varepsilon(1-\varepsilon)\left(\frac{1}{\varepsilon}-1\right)} > c_2(\varepsilon) x^{1-2\varepsilon}.$$

Since $\varepsilon > 0$ is arbitrary, the proof of the lemma is complete.

LEMMA 16. *For any rational prime p, and any $\varepsilon > 0$, we have the estimate*

$$n_k(p) < c_3(\varepsilon) p^{\zeta_k+\varepsilon},$$

with $\zeta_k = \frac{1}{4} e^{\frac{1}{k}-1}$.

Proof. This result is obtained by using the method of I. M. Vinogradov [11], in conjunction with the well-known character sum estimate of Burgess [3]. The proof requires only simple changes.

We can now give a proof of the theorem. The integer k is not assumed to be an odd prime unless stated.

Proof of the theorem. As indicated earlier, we divide the sum which we estimate into three parts. We write

$$\sum_{p<x} (n_k(p))^a = L_1 + L_2 + L_3,$$

where L_1 is defined to be the left hand sum with the extra condition $n_k(p) < M$, where M is an integer. L_2 and L_3 are defined similarly, the extra conditions being respectively

$$M \leqslant n_k(p) < c_2 \log x, \quad \text{and} \quad c_2 \log x \leqslant n_k(p) < x.$$

To estimate L_1 we apply (9) to the relation

$$L_1 = \sum_{q_r < M} q_r^a \sum_{\substack{p<x \\ n_k(p)=q_r}} 1 = \sum_{q_r<M} q_r^a \{S(x; q_1, \ldots, q_{r-1}) - S(x; q_1, \ldots, q_r)\} \tag{15}$$

where $q_1, \ldots, q_r$ are the first r rational primes, and so obtain that

$$L_1 = \sum_{q_r<M} q_r^a \{n_{r-1}^{-1} - n_r^{-1}\} \frac{x}{\log x} + o_M\left(\frac{x}{\log x}\right),$$

as $x \to \infty$. We write o_M to denote that the error term may not tend to zero uniformly with respect to M. By using the estimate

$$n_r > c(k) k^r$$

of Lemma 5, we see that we may extend to infinity in a natural way the series which is the coefficient of the leading term in this expression.

This introduces a further error term which does not exceed

$$O\Big(\frac{x}{\log x} \sum_{q_r \geqslant M} k^{-r} q_r^a\Big) < c_6 \frac{x}{\log x} \exp\Big(-c_5 \frac{M}{\log M}\Big).$$

Here we have used (as earlier) the estimate $q_r = O(r \log r)$ if $r \geqslant 2$. Collecting results we see that, with $C_{k,a}$ defined in the obvious manner,

$$L_1 = C_{k,a} \frac{x}{\log x} + O\left(\frac{x}{\log x} \exp\Big(-c_5 \frac{M}{\log M}\Big)\right) + o_M\left(\frac{x}{\log x}\right), \tag{16}$$

where the first term is uniform with respect to M.

To estimate L_2, we fix our attention upon a particular prime divisor k_1 of k. Then when $q_1, \ldots, q_r$ are kth powers $(\mathrm{mod}\, p)$, they are also k_1th powers $(\mathrm{mod}\, p)$. If k_1 is odd, then we estimate L_2 by beginning as for L_1, but in place of the asymptotic equality (9), we use the inequality (14). We can certainly do this if c_2 is chosen suitably depending only upon k. We then obtain the inequality

$$\begin{aligned} L_2 &< c_7 \sum_{M \leqslant q_r < c_2 \log x} q_r^a \Big(k_1^{-r} \frac{x}{\log x} + x^{1/2}\Big) \\ &= O_\varepsilon\left(\frac{x}{\log x} \exp\Big(-c_8 \frac{M}{\log M}\Big) + x^{1/2+\varepsilon}\right). \end{aligned} \tag{17}$$

If k is a power of 2, so that $k_1 = 2$, then we can use the quadratic reciprocity law in place of Lemmas 10 and 11, and obtain the inequality (17) on the lines of the derivation in Erdös' paper [5].

We now let k be arbitrary, but fixed, once again.

In order to estimate L_3 it is convenient to divide it up into two parts. For convenience, from now until the end of the proof we denote ζ_k by ζ. Let $\nu = \frac{1}{3}(1-\zeta)$, so that the hypotheses of the theorem guarantee that ν is positive. We write $L_3 = L_4 + L_5$, where

$$L_4 = \sum_{\substack{c_2 \log x \leqslant n_k(p) < (\log x)^\nu \\ p<x}} (n_k(p))^a,$$

and L_5 is a similar sum with the condition on $n_k(p)$ replaced by

$$(\log x)^\nu \leqslant n_k(p) < x.$$

Let us first estimate L_4. Let q_s be a prime which satisfies

$$\tfrac{1}{2} c_2 \log x \leqslant q_s < c_2 \log x.$$

Such a prime will exist if x is large enough. Then it is evident from the estimate (14), that if $r \geqslant s$ holds, then when k has an odd prime divisor,

$$S(x; q_1, \ldots, q_r) \leqslant S(x; q_1, \ldots, q_s) = O\left(x^{1/2} + 2^{-s}\frac{x}{\log x}\right)$$
$$= O\left(\frac{x}{\log x}\exp\left(-c_9\frac{\log x}{\log\log x}\right)\right).$$

This result also holds, as in Erdös [5], if k is a power of 2. Using this, we obtain for L_4 the estimate

$$L_4 \leqslant (\log x)^{a\nu} S(x; q_1, \ldots, q_s) < c_{10}x(\log x)^{-2}. \tag{18}$$

Finally, we consider L_5. If $n_k(p) \geqslant y$, then any rational integer made up from primes not exceeding y, must be a kth power residue (mod p). For any $x \geqslant y \geqslant 2$, let us consider the set of such integers not exceeding x^2. Let us denote these by a_i, $i = 1, \ldots, Z$, where $Z = \psi(x^2, y)$. Let p be a prime for which $n_k(p) > y$. Then since the integers $\{a_i\}$ belong to at most $\big((p-1)+1\big)/k$ residue classes (mod p), we see that if $p \geqslant k^2 - k + 1$,

$$p\sum_{r=0}^{p-1}\left(Z(r; p) - \frac{Z}{p}\right)^2 \geqslant \left(1 - \frac{1}{k-1}\right)p^2\frac{Z^2}{p^2}.$$

Thus, the number of primes $p < x$, for which $n_k(p) \geqslant y$, is, by Lemma 8, less than

$$k^2 - k + 1 + 18x^2Z^{-1} < k^2 + 18x^2\{\psi(x^2, y)\}^{-1}.$$

Taking $\delta = \nu^{-1}$ in Lemma 13, we see that if $y \geqslant (\log x)^\nu$ then

$$\psi(x^2, y) > c_{11}(\varepsilon)x^{2(1-\nu)-\varepsilon}.$$

Hence, since Lemma 16 shows that in any case $n_k(p) < c(\varepsilon)p^{\zeta+\varepsilon}$ holds for any fixed $\varepsilon > 0$, we have that

$$L_5 < c_{12}x^{2\nu+\varepsilon}\max_{q_r < c(\varepsilon)x^{\zeta+\varepsilon}} q_r^a < c_{13}x^{2\nu+\varepsilon+\zeta+\varepsilon} < c_{14}x(\log x)^{-2}, \tag{19}$$

since, if ε is small enough,

$$2\nu + \varepsilon + \zeta + \varepsilon < 3\nu + \zeta = 1.$$

Collecting the results (16), (17), (18) and (19) we see that

$$\frac{\log x}{x}\sum_{p<x}\big(n_k(p)\big)^a = C_{k,a} + o_M(1) + O\left(\exp\left(-c_8\frac{M}{\log M}\right)\right).$$

By letting first x, and then M tend to infinity, we see that

$$\lim_{x\to\infty}\frac{\log x}{x}\sum_{p<x}\big(n_k(p)\big)^a$$

exists, and has the value $C_{k,a}$.

This completes the proof of the theorem.

In particular, $4e^{1-1/k} \geqslant 4\sqrt{e} > 1$ so that we may take $a = 1$, and obtain the analogue of Erdös' theorem.

If k is odd, then $n_r = k^r\varphi(k)$, so that

$$C_{k,a} = \frac{k-1}{\varphi(k)}\sum_{r=1}^{\infty}k^{-r}q_r^a,$$

and for odd primes $\varphi(k) = k-1$, giving the value of $C_{k,a}$ stated in the theorem.

Finally, we note that a sharper error term can be obtained in the theorem by using the Siegel-Brauer theorem, (see Brauer [2], Theorem 2, p. 743), for the fields K_r in which we need to apply Lemma 7, are all normal extensions of Q.

References

[1] M. B. Barban, *The 'Large Sieve' method and its applications in the theory of numbers*, Russian Mathematical Surveys 21 (1966), pp. 49-104.

[2] R. Brauer, *On the zeta-functions of algebraic number fields*, Amer. Journ. Math. 72 (1950), pp. 739-746.

[3] D. Burgess, *On character sums and primitive roots*, Proc. Lond. Math. Soc. (3) 12 (1962), pp. 179-192.

[4] H. Davenport and H. Halberstam, *The values of a trigonometrical polynomial at well spaced points*, Mathematika 13 (1966), pp. 91-96.

[5] P. Erdös, *Számelméleti megjegyzések I*, Mat. Lapok. 12 (1961), pp. 10-17.

[6] H. Hasse, *Bericht über Untersuchungen aus Probleme aus der Theorie der algebraischen Zahlkörper. I Klassenkörpertheorie*, Berlin 1928.

[7] — *Das allgemeine Reziprozitätsgesetz und seine Ergänzungssätze in beliebige algebraischen Zahlkörpern für gewisse nicht-primäre Zahlen*, Crelle 153 (1924).

[8] E. Landau, *Über Ideale und Primideale in Idealklassen*, Math. Zeit. 2 (1918), pp. 52-154.

[9] — *Vorlesungen über Zahlentheorie*, Band 3, Leipzig 1927.

[10] G. J. Rieger, *Verallgemeinerung der Siebmethode von A. Selberg auf algebraische Zahlkörper II*. Crelle 201 (1959), pp. 157-171.

[11] I. M. Vinogradov, *On the bounds of the least non-residue of k-th powers*, Trans. Amer. Math. Soc. 29 (1927), pp. 218-226.

[12] E. Weiss, *Algebraic Number Theory*, New York 1963.

[13] O. Zariski and P. Samuel, *Commutative Alegbra*, Vol. 1, New York 1958.

UNIVERSITY OF NOTTINGHAM

Reçu par la Rédaction le 9. 1. 1967