icm©

Therefore there exists $T \leqslant \exp(\exp 3X)$ such that

$$Q(T) \geqslant \frac{c_1}{X^{1/4}} \sum_{\substack{1 \leqslant p \leqslant X/2^{10} \\ p \equiv 1 (\mathrm{mod}\, 4)}} \frac{1}{p^{1/2}} \geqslant c_1 \frac{X^{1/4}}{\ln X}.$$

Hence

$$\underline{\sigma}(T-\eta, T+\eta) \leqslant -c_1 (\ln\ln T)^{1/4-\varepsilon}$$

for $T > T_0(\varepsilon)$ and $\varepsilon > 0$.

(26) is true, (25) follows by the same way, one has to use only the corollary of this lemma.

Remark. If we estimate the degree of linear independence more exactly (Lemma 5) the term $(\ln\ln\lambda)^{1/4-\varepsilon}$ in (25) and (26) can be replaced by $\left(\frac{\ln\ln\lambda}{\ln\ln\ln\lambda}\right)^{1/4}$.

I wish to thank Professor P. Turán for reading the paper and making some valuable suggestions.

References

[1] A. S. Besicovitch, *On the linear independence of fractional powers of integers*, J. London Math. Soc. 15 (1940), pp. 3-6.

[2] H. Bohr and B. Jessen, *One more proof of Kronecker's theorem*, J. London Math. Soc. 7 (1932), pp. 274-275.

[3] A. E. Ingham, *On two classical lattice-points problems*, Proc. Cambridge Phil. Soc. 36 (1940), pp. 131-138.

[4] D. J. Kendall, *On the number of lattice-points inside a random oval*, Quart. Job. Math. (Oxford), 19 (1948), pp. 1-26.

[5] E. Landau, *Vorlesungen über Zahlentheorie*, Leipzig 1927.

[6] P. Turán, *Eine neue Methode in der Analysis und deren Anwendungen*, Budapest 1953.

Reçu par la Rédaction le 19. 2. 1967

ACTA ARITHMETICA
XIV (1968)

Some notes on k-th power residues

by

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

Let k be a positive integer and p a rational prime satisfying $p \equiv 1 \pmod{k}$. We then define $n_k(p)$ to be the least positive integer which is not a kth power $(\mathrm{mod}\, p)$. For the remaining primes we define it to be zero.

It is a long standing conjecture that the estimate $n_k(p) = O(p^\varepsilon)$ holds for any fixed value of $\varepsilon > 0$. In an average sense this result is known to be true since there is a constant c_k for which

$$\sum_{p<x} n_k(p) \sim c_k x/\log x,$$

as $x \to \infty$. For a proof of this result we refer for example to Elliott [5].

If we assume an extended form of the Riemann hypothesis then the method of N. C. Ankeny [1] shows that

$$n_k(p) = O\big((\log p)^2\big).$$

In the other direction, Chowla showed that there is a positive constant c for which $n_2(p) > c\log p$ holds infinitely often. It is our present purpose to show that a similar result holds for certain other values of k.

THEOREM 1. *If k is an odd prime there is a constant $d_k > 0$ for which*

$$n_k(p) > d_k \log p$$

holds infinitely often.

For the duration of this theorem, we assume that k is an odd prime.

We need two lemmas.

For an integer k let Q_k denote the cyclotomic field obtained by adjoining the kth roots of unity to the field of rational numbers Q. Let $\bar{Q}_k$ denote the ring of algebraic integers in this field. For any element a of $\bar{Q}_k$ we use $[a]$ to denote the principal ideal generated in $\bar{Q}_k$ by a. Furthermore we take $\varrho = \exp(2\pi i/k)$ and $\lambda = 1-\varrho$ which are both algebraic integers of $\bar{Q}_k$.

icm©

LEMMA 1. *Let $q_1, q_2, \ldots, q_r$ denote r rational primes, possibly including k. Let p be a rational prime satisfying $p \equiv 1 \pmod k$ which does not divide $q_1 q_2 \ldots q_r$ or k. Then each q is a k-th power $\pmod p$ for each value of i, if and only if any prime ideal $\mathfrak{p}$ dividing p in Q_k belongs to certain ideal classes* mod $[\lambda^2 q_1 \ldots q_r]$.

Proof. Since p satisfies $p \equiv 1 \pmod k$, $[p]$ splits into $\varphi(k) = k-1$ conjugate prime ideals $\mathfrak{p}$. It was shown in [5] that if there are h_r ideal classes mod $[\lambda^2 q_1 \ldots q_r]$ then the above stated result holds if and only if any $\mathfrak{p}$ which divides p belongs to one of $k^{-r} h_r$ of these ideal classes.

LEMMA 2. *Let K be an algebraic number field and $\bar{K}$ its ring of integers. Let $\mathfrak{a}$ be an ideal of $\bar{K}$ which has $h(\mathfrak{a})$ ideal classes. Then the number of prime ideals $\mathfrak{p}$ satisfying $p = N\mathfrak{p} < x$ and belonging to a particular ideal class* $(\bmod\ \mathfrak{a})$, *is at least*

$$x/(N\mathfrak{a})^{c_1} \log x$$

provided only that $x > (N\mathfrak{a})^{c_2} > 1$. Here both constants depend only upon K.

Proof. This result is proved by Fogels [6].

Proof of the theorem. We now take $q_1, \ldots, q_r$ to be the first r rational primes. We count the number of prime ideals $\mathfrak{p}$ which are of the first degree, do not divide $kq_1 \ldots q_r$ and belong to one of the appropriate ideal classes mentioned in Lemma 1. Moreover $\mathfrak{p}$ must divide a rational prime p not exceeding x.

By Lemma 2 the number of these is at least

$$k^{-r} x/(N[\lambda^2 q_1 \ldots q_r])^{c_1} \log x - \sideset{}{'}\sum_{N\mathfrak{p}=p<x} 1, \tag{1}$$

where the final summation is taken over those primes p dividing $kq_1 \ldots q_r$, provided only that x exceeds $(N[\lambda^2 q_1 \ldots q_r])^{c_2}$.

Since the inequalities

$$N[\lambda^2 q_1 \ldots q_r] \leqslant \exp\Big(c_3 \sum_{i \leqslant r} \log q_i\Big) < e^{c_4 q_r} < e^{c_5 r \log r},$$

follow from a well-known estimate, it is enough if we take r to be the integer part of $\varepsilon \log x / \log\log x$ for a small but fixed value of ε.

Clearly

$$\sideset{}{'}\sum_{N\mathfrak{p}=p<x} 1 \leqslant r < \log x$$

so that the expression (1) exceeds

$$\exp(-c_6 r \log r) x (\log x)^{-1} - \log x.$$

This is then positive if ε is sufficiently small.

We thus obtain a prime ideal $\mathfrak{p}$, corresponding to which there is a rational prime p for which

$$n_k(p) > q_r > c_7 r \log r > c_8 \log x.$$

The desired result now clearly follows.

With the above restrictions on p, k we define $r_k(p)$ to be the least positive prime p which is a kth power $(\bmod\ p)$, and to be zero otherwise. It is natural to conjecture that the asymptotic equality

$$\sum_{p<x} r_k(p) \sim e_k x (\log x)^{-1}, \quad \text{as} \quad x \to \infty,$$

holds. We show that this is certainly true if $k = 2$.

THEOREM 2.

$$\sum_{p<x} (r_2(p))^a = g_a L_i(x) + O\left(x \exp\left(-\frac{c \log_2 x}{\log_3 x}\right)\right),$$

where g, c are positive constants, c being arbitrary but fixed, and

$$g_a = \sum_{j=1}^{\infty} 2^{-j} q_j^a,$$

the q_j running through all the rational primes; provided $a < 4$.

Proof. Let $S(k, x; q_r)$ denote the number of primes $p < x$ which satisfy $r_k(p) = q_r$. The sum which we wish to estimate is clearly

$$\sum_{q_r < x} q_r^a S(k, x; q_r).$$

The evaluation of $S(k, x; q_r)$ for small values of q_r is carried out much as the similar calculation used to count the number of primes $p < x$ for which $n_k(p) = q_r$.

We first show that if N is a large, temporarily fixed integer, then uniformly for $q_r \leqslant N$,

$$S(k, x; q_r) = \frac{1}{n_r}\big(1 + o(1)\big)\frac{x}{\log x}, \quad \text{as} \quad x \to \infty, \tag{2}$$

where n_r depends upon the degrees of certain algebraic number fields.

Let $q_1', \ldots, q_s'$ be s primes, then (see [5], Lemma 5), the number of primes $p \leqslant x$, satisfying $p \equiv 1 \pmod k$, for which q_i', $i = 1, \ldots, s$, are kth powers $(\bmod\ p)$ is

$$f_s\big(1 + o(1)\big) x / \log x \quad \text{as} \quad x \to \infty,$$

icm©

where

$$f_s = \begin{cases} k^{-s} & \text{if } k \text{ is odd,} \\ 2^{m_1}k^{-s} & \text{if } 2\|k \text{ and } m_1 \text{ is the number of odd } q_i' \\ & \quad \text{dividing } k \text{ and satisfying } q_i' \equiv 1 \pmod 4, \\ 2^{m_2}k^{-s} & \text{if } 4\|k \ (8|k) \text{ and } m_2 \text{ is the number of} \\ & \quad \text{distinct odd } q_i' \text{ which divide } k. \end{cases}$$

Let us put $f(\mathfrak{q}_s)$ to denote the value of f_s for a specific set of primes $(q_1', \ldots, q_s') = \mathfrak{q}_s$. Then by the exclusion principle, the asymptotic density amongst all primes of those primes for which $r_k(p) > q_r$ is

$$\sum_{s=0}^{r-1}(-1)^s \sum_{\mathfrak{q}_s} f(\mathfrak{q}_s), \tag{3}$$

where the inner sum is over all possible $\mathfrak{q}_s$ formed by the first r primes q_i, and where $f(\mathfrak{q}_0) = 1$.

Suppose that q_r exceeds the maximum prime divisor of k, and, for example, that $2\|k$. Any selection $\mathfrak{q}_s$ is formed by taking a subset of t of the odd prime divisors of k which satisfy $q_i \equiv 1 \pmod 4$ with $0 \leqslant t \leqslant s$, and $s-t$ further primes q_i with $1 \leqslant i \leqslant r$, $q_i \nmid k$.

Let us denote the number of distinct odd prime divisors of k which are $\equiv 1 \pmod 4$ by w. We then have typically

$$f(\mathfrak{q}_s) = 2^t k^{-s},$$

and letting $\mathfrak{q}_s$ run over all the selections of s primes in the inner sum of (3) we obtain

$$\sum_{\mathfrak{q}_s} f(\mathfrak{q}_s) = k^{-s} \sum_{0 \leqslant t \leqslant \min(s,w)} 2^t \binom{w}{t}\binom{r-1-w}{s-t}.$$

The R. H. S. is the coefficient of ζ^s in the binomial expansion of

$$k^{-s}(1+2\zeta)^w(1+\zeta)^{t-1-w}. \tag{4}$$

If ϱ is a real number so that $k\varrho > 1$, then this is

$$\frac{1}{2\pi i}\int_{|\zeta|=\varrho} \zeta^{-1}(1+2\zeta)^w(1+\zeta)^{r-1-w}(k\zeta)^{-s}\,d\zeta,$$

so that the value of the sum in (3) is

$$\frac{1}{2\pi i}\int_{|\zeta|=\varrho} \zeta^{-1}(1+2\zeta)^w(1+\zeta)^{r-1-w}\sum_{s=0}^{r-1}(-k\zeta)^{-s}\,d\zeta.$$

Now we can extend the sum over s to cover all integers $s \geqslant 0$, since the Laurent expansion of (4) has no powers of ζ higher than ζ^{r-1}, and furthermore $|k\zeta|^{-1} = (k\varrho)^{-1} < 1$, so that we obtain for our sum (3) the estimate

$$\frac{1}{2\pi i}\int_{|\zeta|=\varrho} (1+2\zeta)^w(1+\zeta)^{r-1-w}(\zeta+1/k)^{-1}\,d\zeta.$$

The integrand is regular in the whole finite plane save at the point $\zeta = -1/k$, where there is a simple pole with residue

$$(1-2/k)^w(1-1/k)^{r-1-w}.$$

Hence, we have for n_r^{-1} the value

$$(1-1/k)^{r-1-w}(1-2/k)^w\{1-(1-1/k)\} = \{(1-2/k)^w(1-1/k)^{r-1-w}\}/k.$$

This is certainly non-zero unless $k = 2$. In this case $w = 0$, and the above method shows that we have $n_r = 2^r$. If $4\|k$ we replace w by the total number of distinct odd prime divisors of k, provided q_r still exceeds every prime divisor of k. For smaller values of r we obtain an explicit but a somewhat more complicated expression. It is in any case clear that for all $r \geqslant 1$,

$$n_r^{-1} \leqslant (1-1/k)^{r-1}. \tag{5}$$

We next recall that if k is an odd prime, then $q_1, \ldots, q_r$ are non-kth powers $\pmod p$ for primes p, $p \nmid (kq_1 \ldots q_r)$, $p \equiv 1 \pmod k$, if and only if any prime ideal divisor $\mathfrak{p}$ of $[p]$ in $\overline{Q}_k$ belong to $k^{-r}h(\mathfrak{N}_r)$ ideal classes $(\bmod\, \mathfrak{N}_r)$, where $\mathfrak{N}_r = [\lambda^2 q_1 \ldots q_r]$. (Cf. Lemma 1, and also [5], Lemma 12 and following). We can then use a generalization of Selberg's sieve method, and show that for any constant $D > 0$, we have

$$\sum_{\substack{p<x \\ r_k(p)<(\log x)^D}} (r_k(p))^\alpha = g_{k,\alpha}x/\log x + o_N(x/\log x) + O(\Delta(N)x/\log x),$$

where

$$g_{k,\alpha} = \sum_{r=1}^{\infty} q_r^\alpha n_r^{-1} \quad \text{and} \quad \Delta(N) \leqslant \exp(-c_9\sqrt{\log N}),$$

and where $q_1, q_2, \ldots$, is the set of all positive rational primes. (See [4], (15)-(19).) The second error term here is not necessarily uniform with respect to all values of N.

Thus

$$\limsup_{x\to\infty} \frac{\log x}{x}\left|\sum_{\substack{p<x \\ r_k(p)<(\log x)^D}} (r_k(p))^\alpha - g_{k,\alpha}\frac{x}{\log x}\right| \leqslant c_{10}\Delta(N),$$

for all $N > 1$, so that we obtain

$$\sum_{\substack{p<x \\ r_k(p)<(\log x)^D}} (r_k(p))^a \sim g_{k,a} x/\log x,$$

and in order to prove Theorem 2 with k in place of 2, we need only show that there is a constant $D > 0$ (possibly depending upon a), so that

$$(6) \qquad \sum_{\substack{p<x \\ r_k(p)\geqslant(\log x)^D}} (r_k(p))^a = o(x/\log x), \quad \text{as} \quad x\to\infty.$$

We shall do this for $k = 2$. We need the following form of the large sieve of Linnik.

LEMMA 3. *If $0 < a_1 < \ldots < a_Z \leqslant N$ is a set of integers, and $A(N, l, q)$ is the number of these a_i which satisfy $a_i \equiv l \pmod q$, then*

$$\sum_{p\leqslant\sqrt{N}} p \sum_{l=0}^{p-1} \big(A(N, l, p) - p^{-1}Z\big)^2 \leqslant 7ZN.$$

Proof. This result is contained in Theorem 1 of Bombieri [4]. We shall not be concerned with the particular value 7 on the R. H. S. of this inequality.

Let $n_k(p) = q_r$, $r > 1$, then $q_1, \ldots, q_{r-1}$ are all kth powers (mod p), and so therefore are all the integers formed from these q_i. We can then construct a sequence A to which we can apply Lemma 3. However, if $r_k(p) = q_r$ the information that $q_1, \ldots, q_{r-1}$ are not kth powers (mod p) is not quite so easily used, for clearly, some of the products of the q_i might well be kth powers (mod p).

More exactly, let G, G^k denote the group of reduced residue classes (mod p), and the group of kth powers of these classes, respectively. Let Γ_k denote the quotient group G/G^k. Then Γ_k is isomorphic to the additive group of residue classes (mod k). Let us denote the classes of Γ_k by γ_i, $i = 1, \ldots, k$, where for convenience we take $\gamma_k = e$ the identity of Γ_k.

If $\gamma_1, \gamma_2 \in \Gamma_k$ then what we have just said amounts to the fact that $\gamma_1\gamma_2 = e$ or a similar result might hold. If in particular $k = 2$, then clearly $\gamma_1\gamma_2 = e$ so that the product of an odd number of the primes q_i remains a quadratic non-residue (mod p). Let us first deal with this case, which we need for our theorem.

LEMMA 4. *Let $\psi(k, x, y)$ denote the number of integers not exceeding x which are made up of primes $p \leqslant y < x$, and whose total number of prime divisors, counted with multiplicity, is a multiple of k. Then if $h > 1$ and ε are positive constants,*

$$\psi\big(k, x, (\log x)^h\big) > c(\varepsilon)x^{1-1/h-\varepsilon}.$$

Proof. Define the integer t by:

$$y^{kt} \leqslant x < y^{k(t+1)}, \qquad y = (\log x)^h,$$

so that if x is large enough t is non-zero.

Let $\pi(y)$ denote the number of primes not exceeding y, then clearly

$$kt \leqslant \log x/h\log\log x \leqslant \tfrac{1}{2}\pi(y).$$

Now the product of any kt primes $p \leqslant y$ will be of the type desired in our lemma.

Hence we have the inequalities

$$\psi(k, x, y) \geqslant \binom{\pi(y)}{kt} \geqslant \left(\frac{\pi(y)-kt}{kt}\right)^{kt} \geqslant \left(\frac{\pi(y)}{2kt}\right)^{kt} > \left(\frac{y}{4kt\log y}\right)^{kt}$$
$$> x\exp\big(-kt\log(4kt\log y) - \log y\big).$$

Since moreover

$$kt\log(4kt\log y) + \log y < \frac{\log x}{\log y}\log(4\log x) + \log y < \left(\frac{1}{h}+\varepsilon\right)\log x,$$

we obtain the desired result.

We now form the set of integers $a_i \leqslant x^2$ which are made up of the primes $q_1, \ldots, q_{r-1}$, and which have an odd number of prime factors. The number Z of these is clearly at least

$$\psi(2, x^2q_1^{-1}, q_{r-1})$$

so that if $(\log x)^D < q_{r-1} \leqslant 2(\log x)^D$ we see that

$$Z \geqslant \psi\big(2, \tfrac{1}{2}x^2(\log x)^{-D}, (\log x)^D\big) > c(D, \varepsilon)x^{2-2D^{-1}-2\varepsilon}.$$

The integers a_i all belong to $1 + \frac{1}{2}(p-1)$ or fewer classes (mod p), so that if $p \leqslant x$ and $r_2(p) \geqslant q_r$,

$$p\sum_{l=0}^{p-1}\big(A(N, l, p) - p^{-1}Z\big)^2 \geqslant c_{11}Z^2,$$

and therefore

$$\sum_{p\leqslant x, r_2(p)\geqslant(\log x)^D} 1 \leqslant c_{12}x^2/\psi \leqslant c_{13}x^{2D^{-1}+2\varepsilon}.$$

Before we proceed we note that an alternative method of estimating the set of $m \leqslant x$ for which the total number of divisors $\Omega(m)$ is odd, and which are made up of primes $q \leqslant q_r$ is a slight modification of that of A. I. Vinogradov [2]. We see that the number which we wish to investigate is

$$\frac{1}{2}\sum_{m\leqslant x}\big(1-(-1)^{\Omega(m)}\big),$$

where m runs over an obvious set of integers. The method of Vinogradov which we have just referred to gives a good estimate for the number of our m not exceeding x, and depends upon studying the behaviour of the generating function

$$F(s) = \prod_{p\leqslant y} (1-p^{-s})^{-1},$$

as a function of y, s. The terms $(-1)^{\Omega(m)}$ are clearly generated by

$$\prod_{p\leqslant y} (1-p^{-s}) = \frac{1}{F(s)},$$

and so with obvious modifications we can deal with the sum $\sum_{m\leqslant x}(-1)^{\Omega(m)}$ and obtain a sharp estimate for the number of special integers $m \leqslant x$. It is here however not particularly advantageous. To complete the proof of Theorem 2 we appeal to the following result of U. V. Linnik and A. I. Vinogradov [3].

LEMMA 5. *For any* $\varepsilon \geqslant 0$,

$$r_2(p) \ll p^{1/4+\varepsilon}.$$

Proof of Theorem 2. We have already reduced our problem to proving the asymptotic estimate (6). By Lemmas 4 and 5, we see that

$$\sum_{p<x, r_2(p)\geqslant(\log x)^D} (r_2(p))^a \leqslant (c_{14}x^{1/4+\varepsilon})^a \sum_{p<x, r_2(p)\geqslant(\log x)^D} 1 \leqslant c_{15}x^{(1/4+\varepsilon)a+2D^{-1}+2\varepsilon}.$$

Here, if ε is small and D is large, then the exponent of x is

$$\tfrac{1}{4}a+\varepsilon(a+3)+2/D < 1.$$

So that (6) is proved, and insofar as we obtain an asymptotic estimate, so is Theorem 2. To obtain the stated result we can use the law of quadratic reciprocity together with the well-known result of Siegel-Walfisz (Prachar [7], Satz 8.3, p. 144) concerning the distribution of rational primes in arithmetic progressions. We do not give the details since they are straightforward.

It is natural to seek a similar treatment for general k with which to prove (6). A few simple considerations show that the case $k = 2$ is somewhat special. In the general case we have the following problem: consider any set $\gamma_1', \gamma_2', \ldots, \gamma_r'$ of elements from Γ_k, possibly with repetitions. We wish to know if there is a positive integer t so that the product of any t elements from this set is e.

Suppose that we have such an integer. Then

$$(\gamma_1')^{t-1}\gamma_2' = e = (\gamma_1')^t,$$

so that $\gamma_1' = \gamma_2'$, and indeed all of the γ_i' must be the same. Thus we can only find a suitable t when $\gamma_1' = \gamma_2' = \ldots = \gamma_r'$ and then clearly we can take $t = k$.

When $k = 2$, Γ_2 contains only 2 elements so that if $r_2(p) = q_r$, $r > 1$, then $q_1, q_2, \ldots, q_{r-1}$ must all belong to $\gamma_1 \neq e$.

In general, $r_k(p) = q_r$ implies only that at least $(r-1)/(k-1)$ of the primes q_i, $i = 1, \ldots, r-1$, belong to a particular class γ_j. In order to construct a reasonable sequence A to which we can apply Lemma 3 we need a set of primes $q_{j_1}, \ldots, q_{j_s}$ taken from q_i, $i = 1, \ldots, r$, which all belong to the same class γ_j for a large subset of those primes $p \leqslant x$ for which $r_k(p) = q_r$.

If P_2 denotes the cardinality of a set of the former type and P_1 that set of the latter type, simple combinatorial considerations show that we can find a "P_2-set" so that

$$\binom{r}{\left[\frac{r-1}{k-1}\right]} kP_2 \geqslant P_1. \tag{7}$$

We can now apply Lemma 4 to estimate P_2 and so obtain that

$$P_2 \ll x^{2D^{-1}+\varepsilon}$$

provided that $q_r > c_{16}(\log x)^D$.

Much better than this we cannot expect by the above method, since it can be very simply shown that even with no restriction on the number of prime divisors of the integers counted,

$$\psi(k, x, (\log x)^h) \ll x^{1-1/h+\varepsilon}$$

for any $\varepsilon > 0$.

Thus in order to obtain a useful estimate for P_2 we need that $q_r > (\log x)^D$ should be satisfied for some constant $D > 1$.

However, we shall then have that

$$\binom{r}{\left[\frac{r-1}{k-1}\right]} \geqslant \exp(c_{17} r\log r) \geqslant \exp\left(c_{18}(\log x)^D\right) > x^3,$$

so that the estimate of P_1 derived from (7) using the above method is no better than

$$P_1 \leqslant x^3,$$

which is not good enough for our present requirements.

Finally we see from the remarks following the inequality (5) that we may use the method of proof in Theorem 1 to show that the following result holds.

THEOREM 3. *Let k be any positive integer. Then there is a constant $d_k > 0$, so that for an infinite number of primes p the inequality*

$$r_k(p) > d_k \log p,$$

is satisfied.

References

[1] N. C. Ankeny, *The least quadratic non residue*, Annals of Math. 55 (1) (1952), pp. 65-72.

[2] А. И. Виноградов, *О числах с малыми простыми делителями*, ДАН СССР 109(1956), pp. 683-686.

[3] — и Ю. В. Линник, *Гиперэллиптические кривые и наименьший простой квадратный вычет*, ДАН СССР 168 (1966), pp. 259-261.

[4] E. Bombieri, *On the large sieve*, Mathematika 12 (1965), pp. 201-225.

[5] P. D. T. A. Elliott, *A problem of Erdös concerning power residue sums*, Acta Arith. 13 (1967), pp. 131-149.

[6] E. Fogels, *On the distribution of prime ideals*, Acta Arith. 7 (1961), pp. 255-269.

[7] K. Prachar, *Primzahlverteilung*, Berlin 1957.

Reçu par la Rédaction le 8. 5. 1967

ACTA ARITHMETICA
XIV (1968)

Deux remarques concernant l'équirépartition des suites

par

M. MENDÈS FRANCE (Paris)

*"seeker of truth
follow no path
all paths lead where
truth is here"*
e. e. cummings

1. Notations. Soit g un entier supérieur ou égal à 2. On sait que tout nombre entier non négatif n s'écrit de façon unique dans le système à base g sous la forme

$$n = \sum_{p=0}^{\infty} e_p(n) g^p \tag{1}$$

où les applications e_p sont définies sur l'ensemble des entiers non négatifs et prennent leurs valeurs sur l'ensemble $\{0, 1, \ldots, g-1\}$. La somme (1) est finie: à partir du rang $p = p(n) = \left[\frac{\log n}{\log g}\right]$, tous les termes sont nuls.

Soit $c = (c_n)$ une suite de nombres réels: $c \in \boldsymbol{R}^{\boldsymbol{N}}$. On définit l'application f_c: $\boldsymbol{N} \to \boldsymbol{R}$ par

$$f_c(n) = \sum_{p=0}^{\infty} e_p(n) c_p.$$

En particulier, si θ est un nombre réel, on posera $(\theta) = (1, \theta, \theta^2, \ldots)$ et

$$f_{(\theta)}(n) = \sum_{p=0}^{\infty} e_p(n) \theta^p.$$

Dans la suite de cet article, on choisira $g = 2$ $(e_p(n) \in \{0, 1\})$, ceci afin de simplifier l'écriture. Les résultats s'étendent sans difficulté en base g.

2. Résultats obtenus. Nous voulons démontrer les deux résultats suivants:

THÉORÈME A. *Soit φ une fonction réelle définie sur $\boldsymbol{N}$ et tendant vers l'infini. Il existe une suite d'entiers $\Lambda = (\lambda_n) \in \boldsymbol{N}^{\boldsymbol{N}}$ telle que*