[7] T. Nakayama, *On modules of trivial cohomology over a finite group, II*, Nagoya Math. J. 12 (1957), pp. 171-176.

[8] I. Reiner, *Integral representation of cyclic groups of prime order*, Proc. Amer. Math. Soc. 8 (1957), pp. 142-146.

[9] D. S. Rim, *Modules over finite groups*, Ann. of Math. 69 (1959), pp. 700-712.

[10] — *On projective class groups*, Trans. Amer. Math. Soc. 98 (1961), pp. 459-467.

[11] J. P. Serre, *Corps locaux*, Act. Sci. et Ind. 1296, Paris 1962.

[12] R. G. Swan, *Induced representations and projective modules*, Ann. of Math. 71 (1960), pp. 552-578.

[13] — *Periodic resolutions for finite groups*, Ann. of Math. 72 (1960), pp. 267-291.

[14] — *Projective modules over group rings and maximal orders*, Ann. Math. 76 (1962), pp. 55-61.

NAGOYA UNIVERSITY

Reçu par la Rédaction le 13. 12. 1963

ACTA ARITHMETICA
IX (1964)

Remark concerning integer sequences

by

K. F. Roth (London)

It seems highly plausible that there are various limitations to the extent to which a sequence of natural numbers can be well-distributed simultaneously among and within all congruence classes; unless the sequence is in some sense "nearly" the sequence of all natural numbers or the empty sequence. Many conjectures of this type appear to be very intractable, particularly those closely related to the well-known conjecture that every sequence of positive upper asymptotic density contains arbitrarily long arithmetic progressions. The object of this note is to remark that, on the other hand, a very simple argument yields at least some information concerning irregularities of distribution of an arbitrary sequence with respect to congruence classes. The theorem below is representative of the type of result that can be proved in this way.

THEOREM. *Let N be a natural number and let $\mathcal{N}$ be a set of distinct natural numbers not exceeding N. For any natural number $m \leqslant N$ and any congruence class h modulo q, we denote by $\Phi_{q,h}(\mathcal{N};\, m)$ the number of elements of $\mathcal{N}$ which do not exceed m and lie in the congruence class; and we denote by $\Phi^*_{q,h}(\mathcal{N};\, m)$ the corresponding "expectation", namely*

$$\Phi^*_{q,h}(\mathcal{N};\, m) = \eta\Phi_{q,h}(\mathcal{I};\, m)$$

where $\mathcal{I}$ is the set $\{1, 2, \ldots, N\}$ and

$$\eta = N^{-1}\sum_{\substack{n=1\\ n\in\mathcal{N}}}^{N} 1. \tag{1}$$

For each m, and every natural number q, we define

$$V_q(m) = \sum_{h=1}^{q}\{\Phi_{q,h}(\mathcal{N};\, m) - \Phi^*_{q,h}(\mathcal{N};\, m)\}^2. \tag{2}$$

Then, for all natural numbers Q,

$$\sum_{q=1}^{Q} q^{-1}\sum_{m=1}^{N} V_q(m) + Q\sum_{q=1}^{Q} V_q(N) \gg \eta(1-\eta)Q^2N, \tag{3}$$

where the implicit constant is absolute.

In particular, on choosing $Q = [N^{1/2}]$, *we obtain the existence of a pair* m_0, q_0, *with* $q_0 \leqslant N^{1/2}$, *such that*

$$q_0^{-1} V_{q_0}(m_0) \geqslant \eta(1-\eta) N^{1/2}. \tag{4}$$

Clearly, this theorem exhibits a limitation to the possible accuracy of approximations of the type

$$\Phi_{q,h}(\mathcal{N};\, m) = \eta q^{-1} m + \Delta(q, m)$$

if these are to be valid for all congruence classes of modulus $q \leqslant Q$, and for all $m \leqslant N$.

Proof of the theorem. The inequality (3) holds trivially when $Q = 1$ (although this case is of no significance). We suppose throughout that $Q \geqslant 2$, and write

$$Q_1 = [\tfrac{1}{2}Q]. \tag{5}$$

For all integers n, we denote by $\varkappa(n)$ the characteristic function of $\mathcal{N}$ and by $\varkappa^*(n)$ the corresponding "expectation"; so that

(i) $\varkappa(n) = 1$ if $n \in \mathcal{N}$ and $\varkappa(n) = 0$ otherwise,

(ii) $\varkappa^*(n) = \eta$ if $1 \leqslant n \leqslant N$ and $\varkappa^*(n) = 0$ otherwise.

For any integers q, h, u, v satisfying $q \geqslant 1$ and $u \leqslant v$, we write

$$D_{q,h}(u, v) = \sum_{\substack{n=u \\ n \equiv h \pmod{q}}}^{v} \big(\varkappa(n) - \varkappa^*(n)\big). \tag{6}$$

We note that (2) may now be written in the form

$$V_q(m) = \sum_{h=1}^{q} \{D_{q,h}(1, m)\}^2. \tag{7}$$

We use α, β to denote real numbers and $e(\alpha)$ to denote $e^{2\pi i\alpha}$. Let

$$S(\alpha) = \sum_{n=1}^{N} \big(\varkappa(n) - \varkappa^*(n)\big) e(n\alpha), \tag{8}$$

$$F(\beta) = \sum_{l=0}^{Q_1-1} e(l\beta), \tag{9}$$

where the natural number Q_1 is defined by (5). We shall prove (3) by comparing upper and lower estimates for the expression

$$E = \int_0^1 \sum_{q=1}^{Q} |F(q\alpha) S(\alpha)|^2 d\alpha. \tag{10}$$

To obtain a lower estimate for E, we use the fact that

$$\sum_{q=1}^{Q} |F(q\alpha)|^2 \geqslant \left(\frac{2}{\pi} Q_1\right)^2, \tag{11}$$

for all α. This fact is established by noting that if $|\beta| \leqslant Q^{-1}$ (so that $|Q_1\beta| \leqslant \frac{1}{2}$), we have

$$|F(\beta)| = Q_1 \left|\frac{\sin \pi Q_1 \beta}{\pi Q_1 \beta}\right| \left|\frac{\pi\beta}{\sin \pi\beta}\right| \geqslant \frac{2}{\pi} Q_1;$$

and that corresponding to every real α, there exists an integer q, satisfying $1 \leqslant q \leqslant Q$, and an integer h, such that $|q\alpha - h| \leqslant Q^{-1}$.

On substituting (11) in (10) and noting that

$$\int_0^1 |S(\alpha)|^2 d\alpha = \sum_{n=1}^{N} \big(\varkappa(n) - \varkappa^*(n)\big)^2 = \eta(1-\eta)N,$$

we obtain the estimate

$$E \geqslant \eta(1-\eta) Q^2 N. \tag{12}$$

Now

$$F(q\alpha) S(\alpha) = \sum_{a=1}^{N+q(Q_1-1)} \nu_q(a) e(a\alpha), \tag{13}$$

where

$$\nu_q(a) = D_{q,a}\big(a - q(Q_1-1), a\big). \tag{14}$$

Accordingly,

$$E = \sum_{q=1}^{Q} E_q, \quad \text{where} \quad E_q = \sum_a \nu_q^2(a). \tag{15}$$

Interpreting $D_{q,h}(u, v)$ to be zero when $u > v$, we have

$$\begin{aligned} \nu_q^2(a) &= \{D_{q,a}(1, a) - D_{q,a}(1, a - qQ_1)\}^2 \\ &\leqslant 2\{D_{q,a}(1, a)\}^2 + 2\{D_{q,a}(1, a - qQ_1)\}^2. \end{aligned}$$

But

$$\sum_{a=N+1}^{N+q(Q_1-1)} \{D_{q,a}(1, a)\}^2 = \sum_{a=N+1}^{N+q(Q_1-1)} \{D_{q,a}(1, N)\}^2 \leqslant Q_1 V_q(N),$$

and hence

$$E_q \leqslant 4 \sum_{a=1}^{N} \{D_{q,a}(1, a)\}^2 + 2Q_1 V_q(N).$$

Thus, since

$$D_{q,a}(1, a) = D_{q,a}(1, a+j) \quad \text{for} \quad j = 0, 1, \ldots, q-1,$$

we have

$$E_q \leqslant 4\sum_{h=1}^{q}\sum_{\substack{a=1\\ a\equiv h\,(\mathrm{mod}\,q)}}^{N} q^{-1}\sum_{j=0}^{q-1}\{D_{q,h}(1,a+j)\}^2+2Q_1V_q(N)$$

$$\leqslant 4q^{-1}\sum_{m=1}^{N}V_q(m)+(2Q_1+4)\,V_q(N)$$

$$\ll q^{-1}\sum_{m=1}^{N}V_q(m)+QV_q(N).$$

In view of (15) we see that this estimate in conjunction with (12) yields (3).

UNIVERSITY COLLEGE, LONDON

Reçu par la Rédaction le 20. 12. 1963

ACTA ARITHMETICA
IX (1964)

Rational zeros of two quadratic forms

by

H. P. F. Swinnerton-Dyer (Cambridge)

1. Let f, g be homogeneous quadratic forms in 13 variables, defined over the rationals. Mordell [3] has shown that f and g have a common non-trivial rational zero, provided that they satisfy certain conditions of a non-number-theoretic nature. In this paper I prove the corresponding result for forms in 11 variables:

THEOREM. *Let f, g be homogeneous quadratic forms in* 11 *variables, defined over the rationals; and suppose that for all real λ, μ not both zero the form $\lambda f+\mu g$ is indefinite. Then f and g have a non-trivial common rational zero.*

We shall see in § 2 that the condition of the theorem is the natural one. Henceforth, in discussing functions homogeneous in a set of variables, we shall implicitly assume that the variables are not all zero; in fact it will be convenient to state part of the argument in the language of projective geometry.

The idea of Mordell's proof is as follows. We arrange that f is non-singular and has signature between -3 and 3 inclusive; then by a change of variables it can be written in the form

$$f = \sum_{i=1}^{5} x_i x_{i+5} + f_1(x_{11}, x_{12}, x_{13}). \tag{1}$$

By putting $x_i = 0$ for $6 \leqslant i \leqslant 13$ we ensure that $f = 0$ and we reduce g to a form $g_1(x_1, \ldots, x_5)$ in five variables. We can certainly find a rational zero of g_1 — and thereby a common rational zero of f and g — if g_1 is indefinite. But the possibility of making g_1 indefinite depends only on real and not on rational conditions; for if we have any real transformation of variables which takes f into the form (1) then we can find a rational transformation as close as we like to it which also takes f into the form (1).

If we apply the analogous argument to a pair of forms in 11 variables, we arrive at a form g_1 in only four variables. This may not have a zero