ON INTERVALS CONTAINING AN AFFINELY EQUIVALENT
SET OF n INTEGERS MOD k

L. J. MORDELL

1. Let \( n > 2 \) be a given positive integer and \((x) = (x_1, x_2, \ldots, x_n)\)
a given set of \( n \) integers. Let \( k \) be a given positive integer. Then
L. Redei [1], improving an old result of Thue [2], has recently proved the

**Theorem.** If \( k \) is a prime, there exist integers \( a, b, (a, k) = 1 \), such
that a set of integers \((y)\), defined by

\[
y_r = ax_r + b \pmod{k} \quad (r = 1, 2, \ldots, n),
\]

lies in an interval of width \( L \) where

\[
nL^{n-1} \leq 2^{n-1}k^{n-2},
\]
i.e.

\[
|y_r - y_s| \leq L \quad (r, s = 1, 2, \ldots, n).
\]

The estimate is trivial if it can give a value of \( L \geq k \), i.e. if \( nk^{n-1} \leq 2^{n-1}k^{n-2} \) or \( k \leq 2^{n-1}/n \). There is also a trivial result \( L = 0 \) if we had
allowed \( a \equiv 0 \pmod{k} \).

I notice that Redei's proof can be presented in a rather simpler form and also extended to the case where \( k \) is not a prime. We have now

**Theorem I.** Let \( \delta \) be the greatest divisor of \( k \) such that

\[
x_1 \equiv x_2 \equiv \cdots \equiv x_n \pmod{\delta},
\]

and so \( \delta = (x_1 - x_n, x_2 - x_n, \ldots, x_{n-1} - x_n, k) \). Then integers \( a \neq 0 \pmod{k} \), \( b \) exist such that an integer set \((y)\), defined by

\[
y_r = ax_r + b \pmod{k} \quad (r = 1, 2, \ldots, n),
\]
lies in an interval of width \( L = L(\delta, k) \), where

\[
nL^{n-1} \leq 2^{n-1}\delta k^{n-2}.
\]

There is no loss of generality in theorems of this kind, if we suppose hereafter that \( \delta = 1 \). For clearly

\[
L(\delta, k) = \delta L(1, k/\delta),
\]
since \( y_r - y_s \equiv a(x_r - x_s) \pmod{k} \), and so we can put \( y_r = \delta y'_r + c \) where

Presented to the Society, September 5, 1953; received by the editors April 5, 1953.

854
\( y_r' \) is an integer and \( c \) is a constant.

Results of this kind can also be found by an application of Dirichlet’s classical distribution result and this leads to

**Theorem II.** Let \( \lambda \) be the least positive integer which satisfies the inequality

\[
(\lambda + 1)^n - \lambda^n \geq k^{n-2}.
\]

Then we can take \( L = 2\lambda \) or \( L = 2\lambda + 1 \) according as the inequality or equality sign holds. Under certain conditions, as stated in Theorem III, the result \( L = 2\lambda + 1 \) is best possible.\(^1\)

Further the result \( L = 2\lambda \) can be replaced by \( L = 2\lambda - 1 \) if now \( \lambda \) is the least positive integer which satisfies the inequality

\[
(\lambda + 1)^n - (\lambda - 1)^n \geq 2k^{n-2}.
\]

Write \((k^{n-2}/n)^{(1/(n-1)} = I + f\), where \( I \) is an integer and \( 0 \leq f < 1 \). When \( 0 \leq f < 1/2 \), the result of Theorem I is included in the first part above. For on putting \( \lambda + 1/2 = \mu \), the first inequality is satisfied by \( \lambda + 1/2 \geq I + f \), i.e. \( \lambda = I \) and so \( L = 2I \). Theorem I gives \( L = [2I + 2f] = 2I \).

When \( 1/2 \leq f < 1 \), the result of Theorem I is given in the second part above. For the second equality is satisfied by \( \lambda \geq I + f \), i.e. \( \lambda = I + 1 \) and so \( L = 2I + 1 \). Theorem I, however, gives \( L = [2I + 2f] = 2I + 1 \).

2. For Theorem I, put

\[
y_r = ax_r + b + k\xi_r \quad (r = 1, 2, \ldots, n),
\]

where \( \xi_r \) is an integer. Then we have to satisfy

\[
| a(x_r - x_s) + k(\xi_r - \xi_s) | \leq L \quad (r, s = 1, 2, \ldots, n).
\]

Write

\[
\xi_r = \eta_r + \xi_n, \quad x_r = x_r' + x_n,
\]

where now, and in the remainder of this chapter, \( r \) and \( s \) take the values \( 1, 2, \ldots, n-1 \). Then

\[
| ax_r' + k\eta_r | \leq L, \quad | a(x_r' - x_s') + k(\eta_r - \eta_s) | \leq L.
\]

Define an \((n-1)\)-dimensional region \( R \) by

---

\(^1\) Redei [1, p. 81] states that this is easily proved when \( k \) is a prime and \( n = 3 \). The referee notes that this is obvious even when \( k \) is not a prime on taking \( x_1 = 1, x_2 = 3\lambda + 2, x_3 = 0 \). I should like to thank him for this remark and also for some other valuable comments.
Then $R$ contains a point $(x)$ with coordinates
\[ x_r = ax'_r + k\eta_r \quad (r = 1, 2, \ldots, n - 1), \]
where $a$ and the $\eta$ are integers. We define a $(2n - 1)$-dimensional region $S$ by combining $R$ and
\[ |X_r - ax'_r - k\eta_r| < 1, \quad |a| < k, \]
where the $\eta$ and $a$ are the additional $n$ variables.

We use Minkowski's convex region theorem to find $L$ such that $S$ contains an integer set $[(X), a, (\eta)] \neq [(0), 0, (0)]$. Redei states that the content of $R$ is obviously $nL^{n-1}$, but a proof is contained in the lemma following. Then clearly on integrating first for $\eta$ and $a$, the content $V$ of $S$ is given by
\[ V = nL^{n-1}(2/k)^{n-1}k, \]
and so $V \geq 2^{2n-1}$ if
\[ nL^{n-1} \geq 2^{n-1}k^{n-2}. \]
This is really Redei's result; and on noting the equation defining $R$, it suffices to take
\[ L = (2^{n-1}k^{n-2}/n)^{1/(n-1)}, \]
where the square bracket denotes the integer part. Then $S$ contains an integer set and for this, obviously,
\[ X_r - ax'_r - k\eta_r = 0, \]
i.e.
\[ X_r \equiv ax'_r \pmod{k}. \]

It remains only to show that the trivial result $a = 0$ has been excluded. If $a = 0$, $X_r \equiv 0 \pmod{k}$. By Minkowski's theorem, all the $X_r$ are not zero, since if they were, all the $\eta_r$ would be zero. Hence the trivial solution is excluded if $L < k$, i.e. $k > 2^{n-1}/n$.

3. Theorem II follows from a simple application of a general principle. Let a bounded $n$-dimensional convex region $R(\lambda)$, symmetrical about the origin, be defined by $f(X) \leq \lambda$, where $f(X)$ is a distance function and so $f(X' - X'') \leq f(X') + f(X'')$, and $\lambda$ is a positive parameter. We find an estimate for $L$ such that the region $R(L)$ will contain an integer set $(X) \neq 0$, satisfying $r$ given linear homogeneous congruences $(\pmod{k})$, say,
\[ L_1(X) \equiv 0, L_2(X) \equiv 0, \ldots, L_r(X) \equiv 0. \]
Let \( N(\lambda) \) be the number of lattice points in \( R(\lambda) \). Then if \( (X) \) runs through these \( N(\lambda) \) points, the \( L \)'s assume \( N(\lambda) \) sets of residues \((\text{mod } k)\). If \( N(\lambda) > k^r \), two different lattice points \( (X'), (X'') \) give the same set of residues for the \( L \)'s. Hence \( (X) = (X' - X'') \) satisfies the homogeneous congruences and clearly lies in the region \( R(2\lambda) \).

The \( R(2\lambda) \) may sometimes be improved to \( R(2\lambda - 1) \) as follows. The region \( R(\lambda - 1) \) contains \( N(\lambda - 1) \) lattice points. We adjoin to these, say, \( N_1(\lambda) \) lattice points lying in \( R(\lambda) \) and not in \( R(\lambda - 1) \), taken in such a way that \( (X' - X'') \) does not lie on the boundary of \( R(2\lambda) \). Then if \( N(\lambda - 1) + N_1(\lambda) > k^r \), the point \( (X' - X'') \) will lie in \( R(2\lambda - 1) \). In fact, we take \( N_1(\lambda) = 1 \) in the proof of Theorem II.

4. We require the

**Lemma.** Let \( R(\lambda) \), where \( \lambda \) is a positive integer, denote the region

\[
\left| x_r \right| \leq \lambda, \quad |x_r - x_s| \leq \lambda \quad (r, s = 1, 2, \cdots, n - 1).
\]

Then \( R(\lambda) \) contains exactly

\[
N(\lambda) = (\lambda + 1)^n - \lambda^n
\]

lattice points, i.e. points with integer coordinates.

My original proof was rather lengthy so I replace it by a very simple one found subsequently by Dr. Cassels and kindly put at my disposal. Write \( x_0 = 0 \) and define \( y_0, y_1, \cdots, y_{n-1} \) by \( y_0 = \max (x_r), y_r + x_r = y_0 \) \((r = 1, 2, \cdots, n - 1)\). If \( y_0 \) arises from an \( x_r \), then \( y_s = 0 \). Also \( 0 \leq y_r \leq \lambda \). Then the \( y \)'s can take all integer values satisfying

\[
\max y_r \leq \lambda, \quad \min y_r = 0 \quad (r = 0, 1, 2, \cdots, n - 1).
\]

The first inequality gives \((\lambda + 1)^n\) possibilities for the \( y \)'s, and the second excludes \( y_r = 1, 2, \cdots, \lambda \), i.e. \( \lambda^n \) possibilities. Hence the result.

**Corollary.** It follows on inscribing \((n - 1)\)-dimensional cubes of sides \(1/\lambda\) in \( R \) that the content \( V \) of \( R(1) \) is given by

\[
V = \lim_{\lambda \to \infty} N(\lambda)/\lambda^{n-1} = n.
\]

5. We now find \( \lambda \) so that the region \( R(\lambda) \) contains an integer set \( (X) \) congruent \text{mod } k to at least one of the sets \((ax')\), where \( (x') \) is any given set of \( n - 1 \) integers with \((x'_1, x'_2, \cdots, x'_{n-1}, k) = 1\), and \( a \) takes the values \(1, 2, \cdots, k-1\), i.e.

\[
X_r \equiv ax'_r \pmod k \quad (r = 1, 2, \cdots, n - 1).
\]

Write \( Y_r = X_r - ax'_r \). When \( (X) \) runs through the \( N(\lambda) \) lattice
points in \( R(\lambda) \) and \( a \) runs through the values 0, 1, \cdots, \( k-1 \), then the \( (Y) \) runs through \( kN(\lambda) \) residue sets mod \( k \). Hence if \( kN(\lambda) > k^{n-1} \), there must be at least two different sets \( (X', a') \), \( (X'', a'') \) giving the same residue sets for \( (Y) \). Then a solution of the congruences \( (Y) \equiv 0 \) is given by \( (X) = (X' - X'') \), \( a = a' - a'' \). This set \( (X) \) will be in \( R(2\lambda) \). If this occurs with the trivial solution \( a = 0 \), then \( (X) \equiv 0 \) (mod \( k \)), and so this will be excluded if \( k > 2\lambda \). Hence if \( \lambda \) is a positive integer such that

\[
(\lambda + 1)^n - \lambda^n > k^{n-2},
\]

\( (X) \) will be in the region \( R(2\lambda) \).

If, however, there exists a positive integer \( \lambda \) such that

\[
(\lambda + 1)^n - \lambda^n = k^{n-2},
\]

we show that there will be a suitable point \( (X) \) in \( R(2\lambda + 1) \). For, take a lattice point \( (\bar{X}) \) lying in \( R(\lambda + 1) \) but not in \( R(\lambda) \). This one combined with those in \( R(\lambda) \) gives more than \( k^{n-2} \) sets of residues. But now the solution \( (X) = (X' - X'') \) will lie in \( R(2\lambda + 1) \).

We prove now the

**Theorem III.** The result \( R(2\lambda + 1) \) is best possible if the values assumed by \( (X) - a(x) \) form a complete set of residues mod \( k \) when \( (X) \) runs through the lattice points of \( R(\lambda) \) and \( a \) takes the values 0, 1, 2, \cdots, \( k-1 \).

It suffices to prove that if \( (X) \) is any lattice point in \( R(2\lambda) \), then

\[
(X) = (Z) + (Z'),
\]

where \( (Z) \) and \( (Z') \) are lattice points in \( R(\lambda) \). For then the condition in the theorem implies that the relation

\[
(Z) - a(x) \equiv -(Z')
\]

holds only when \( a = 0 \), \( (Z) = -(Z') \). Then \( (X) = 0 \), and so the only solution of \( (X) \equiv a(x) \), where \( (X) \) is in \( R(2\lambda) \), is the trivial one.

Let \( \alpha, \alpha', \cdots; \beta, \beta', \cdots; \gamma, \gamma', \cdots \) typify indices 1, 2, \cdots, \( n-1 \) for which

\[
X_\alpha = 2Y_\alpha \equiv 0 \pmod{2}, \quad X_\beta = 2Y_\beta - 1 \equiv 1 \pmod{2}, \quad X_\gamma = 2Y_\gamma + 1 \equiv 1 \pmod{2}, \quad X_0 = 0, \quad X_\gamma \leq 0, \quad X_\gamma \geq 0.
\]

When the same argument applies to both the \( \beta \) and \( \gamma \) sets, we use the letter \( \delta \) and put

\[
X_\delta = 2Y_\delta + \epsilon_3, \quad \epsilon_3 = \epsilon_3' = \cdots = \pm 1.
\]
We take \((Z), \,(Z')\) to be lattice points which we can write as
\[
(Z) = (Y_\alpha, \ldots, Y_\beta - 1, \ldots, Y_\gamma \ldots), \quad \text{and} \quad (Z') = (Y_\alpha, \ldots, Y_\beta, \ldots, Y_\gamma + 1, \ldots),
\]
where the notation indicates the various types of coordinates. These points will be in \(R(\lambda)\), i.e. \(|Z_r| \leq \lambda, |Z_r - Z_s| \leq \lambda\), etc., if the following five sets of conditions are satisfied.

(1) \[ |Y_\alpha| \leq \lambda, \quad |Y_\delta| \leq \lambda - 1. \]

These hold, as follows from
\[
|2Y_\alpha| \leq 2\lambda, \quad 2Y_\delta + \epsilon_\delta \leq 2\lambda.
\]
For \(2|Y_\delta| + 1 \leq 2\lambda, \quad |Y_\delta| \leq \lambda - 1/2\), and since \(Y_\delta\) is an integer, \(|Y_\delta| \leq \lambda - 1\).

(2) \[ |Y_\alpha - Y_\alpha'| \leq \lambda, \quad |Y_\delta - Y_\delta'| \leq \lambda. \]

This holds since
\[
|2Y_\alpha - 2Y_\alpha'| \leq 2\lambda, \quad |2Y_\delta + \epsilon_\delta - (2Y_\delta' + \epsilon_\delta')| \leq 2\lambda, \quad \epsilon_\delta = \epsilon_\delta'.
\]
Now \(|2Y_\alpha - 2Y_\beta + 1| \leq 2\lambda\) which gives
\[
|2Y_\alpha - 2Y_\beta + 2| \leq 2\lambda + 1, \quad |2Y_\alpha - 2Y_\beta| \leq 2\lambda + 1,
\]
\[
|Y_\alpha - Y_\beta + 1| \leq \lambda + 1/2, \quad |Y_\alpha - Y_\beta| \leq \lambda + 1/2, \quad \text{etc.}
\]

(3) \[ |Y_\beta - 1 - Y_\gamma| \leq \lambda. \]

This results from
\[
|2Y_\beta - 1 - 2Y_\gamma - 1| \leq 2\lambda,
\]

(5) \[ |Y_\alpha - Y_\gamma| \leq \lambda, \quad |Y_\alpha - Y_\gamma - 1| \leq \lambda. \]

This follows from
\[
|2Y_\alpha - 2Y_\gamma - 1| \leq 2\lambda,
\]
which gives
\[
|2Y_\alpha - 2Y_\gamma| \leq 2\lambda + 1, \quad |2Y_\alpha - 2Y_\gamma - 2| \leq 2\lambda + 1, \quad \text{etc.}
\]

This finishes the proof.

**Bibliography**


**St. Johns College, Cambridge University**