On bases for the set of integers.

By N. G. DE BRUIJN, Delft (Holland).

§ 1. Introduction.

A set of integers $\{b_1, b_2, b_3, \ldots\}$ will be called a base for the set of all integers (shortly: a *base*), whenever any integer x can be expressed uniquely in the form

$$x = \sum_{i=1}^{\infty} \varepsilon_i b_i \qquad (\varepsilon_i = 0 \text{ or } 1, \sum_{i=1}^{\infty} \varepsilon_i < \infty). \tag{1.1}$$

It is not difficult to see that a base is obtained by taking $b_i = \pm 2^{i-1}$ such that both $+$ and $-$ occur infinitly often.

T. SZELE conjectured that any base has the property that it contains just one odd number, just one odd multiple of 2, just one odd multiple of 4, etc.. This will be proved below. It follows that any base can be rearranged in the form $\{d_1, 2d_2, 2^2d_3, \ldots\}$, where the d_i are odd numbers. The sequence $[d_1, d_2, d_3, \ldots]$ shall be called a basic sequence, whenever $\{d_1, 2d_2, 2^2d_3, \ldots\}$ is a base.

It seems to be very difficult to determine all basic sequences. We shall give some necessary and some sufficient conditions for a sequence to be basic. There is, however, one general case which can be dealt with more or less satisfactory (§ 3): If the sequence $[d_1, d_2, \ldots]$ is periodic, i. e. if $d_{i+s} = d_i$ for some $s > 0$ and all i then we can determine in a finite number of steps whether the sequence is or is not basic The case $s = 1$ is trivial, the case $s = 2$ will be studied in some detail (§ 4).

T. SZELE also conjectured that any basic sequence contains ± 1 infinitly often. By studying periodic sequences we could, however, construct examples containing no terms ± 1 at all. For instance, the sequence $[13, -7, 13, -7, 13, -7, \ldots]$ will be shown to be basic. It is remarkable that, for the corresponding base $\{13, -7.2, 13.2^2, \ldots\}$ the decomposition (1.1) can involve large components for small values of x:

$$1 = 13 + 13.2^2 + 13.2^6 - 7.2^7,$$
$$10 = -7.2 - 7.2^3 + 13.2^4 - 7.2^7 + 13\;2^8 - 7\;2^9 + 13\;2^{10} + 13\;2^{12} + 13.2^{16} - 7.2^{17}.$$

In § 5 we shall discuss some generalisations and some related unsolved problems.

We are indebted to DR. A. RÉNYI for some valuable remarks, and to MR. H. J. SCHUTTE for verifying the numerical material listed at the end of § 4.

§ 2. Bases and basic sequences.

We first prove SZELE's conjecture:

Lemma 1. *If $\{b_1, b_2, b_3, \dots\}$ is a basis, then one of the b's is odd and all others are even.*

Proof. At least one of the b's is odd, for otherwise (1.1) is impossible for x odd. The numeration being irrelevant, the lemma can be proved by showing that $b_1 b_2$ is even.

Let V_1 be the set of those integers n for which, in (1.1), $\varepsilon_1 = 0$; V_2 the set with $\varepsilon_2 = 0$, W the set with $\varepsilon_1 = \varepsilon_2 = 0$.

Consider two integers x, y, with $x - y = b_1$. First assume $y \in V_1$, then we have

$$y = \sum_2^\infty \varepsilon_i(y)\, b_i \text{ and hence } x = b_1 + \sum_2^\infty \varepsilon_i(y) b_i.$$

Since the representation of x is unique, we infer that x does not belong to V_1. On the other hand, if $\varepsilon_1(x) = 1$, we find $\varepsilon_1(y) = 0$. Hence, just one of the numbers x, y belongs to V_1.

Now if $x \in V_1$, we immediately deduce that $x + 2b_1$ and $x - 2b_1$ belong to V_1. Hence V_1 is periodic mod $2b_1$. Analogously V_2 is periodic mod $2b_2$. It follows that $W = V_1 \cap V_2$ is periodic mod $2b_1 b_2$. The least positive period of W be denoted by P.

Let, for $\lambda = 0$ or 1, $\mu = 0$ or 1, $W_{\lambda\mu}$ denote the set of integers for which $\varepsilon_1 = \lambda$, $\varepsilon_2 = \mu$. Clearly, $W_{\lambda\mu}$ can be obtained from $W = W_{00}$ by translation. Let K be the number of integers of W which are >0 and $\leqq P$. It follows that any of the sets $W_{00}, W_{01}, W_{10}, W_{11}$ contains exactly K numbers in a period. These sets are mutually disjoint; their union is the set of all integers. Consequently $P = 4K$.

It follows that 4 divides $2b_1 b_2$; hence either b_1 or b_2 is even.

Theorem 1. *Any base can, by rearrangement, be written in the form*

$$\{d_1, 2d_2, 2^2 d_3, \dots\} \tag{2.1}$$

where the numbers d_i are odd.

Proof. Let $\{b_1, b_2, \dots\}$ be a base. By the lemma, we may suppose b_1 to be odd, and $b_2, b_3, \dots$ to be even. Now $\{b_2, b_3, \dots\}$ is a base for the set of even numbers, and so $\{\frac{1}{2}b_2, \frac{1}{2}b_3, \dots\}$ is a base for the integers. Again, one of its elements must be odd, etc..

As stated in § 1, a sequence $[d_1, d_2, \dots]$ of odd numbers will be called basic, whenever (2.1) is a base. The problem as to which odd sequences are basic, has the nature of a convergence problem. Namely, if $d_1, d_2, d_3, \dots$ are given odd numbers, any integer x can be formally developed into a series, analogous to HENSEL's p-adic expansions:

$$x=\sum_{i=1}^{\infty} \varepsilon_i d_i 2^{i-1} \quad (\varepsilon_i = 0 \text{ or } 1, \sum_{1}^{\infty} \varepsilon_i \leqq \infty). \tag{2.2}$$

Here the ε_i are uniquely determined by x, and (2.2) has to be interpreted as follows: for any $k \geqq 1$ we have

$$x=\sum_{i=1}^{k} \varepsilon_i d_i 2^{i-1} \equiv 0 \pmod{2^k}. \tag{2.3}$$

Clearly, the sequence $[d_1, d_2, d_3, \dots]$ is basic whenever $\sum_{1}^{\infty} \varepsilon_i < \infty$ for all x.

It is easily proved that, if d_1 is odd, $[d_1, d_2, d_3, \dots]$ is basic if and only if $[d_2, d_3, \dots]$ is basic. Hence we have

Theorem 2. *A basic sequence remains basic whenever a finite number of odd numbers is added, omitted or changed into other odd numbers.*

The following rather trivial negative criteria are immediate consequences:

Theorem 3. *If all but a finite number of the d's are of like sign, then the sequence $[d_1, d_2, \dots]$ is not basic*

If all but a finite number of the d's are divisible by one and the same prime number, the sequence $[d_1, d_2, \dots]$ is not basic.

Owing to theorem 2 we may assume that there are no exceptions at all; in that case both results are trivial.

A negative criterion of a different kind is

Theorem 4. *If we have, for all large k,*

$$|d_k| > \frac{|d_{k-1}|}{2} + \frac{|d_{k-2}|}{2} + \dots + \frac{|d_1|}{2^{k-1}} + \frac{1}{2}, \tag{2.4}$$

then $[d_1, d_2, \dots]$ is not basic.

Proof. Assume $[d_1, d_2, \dots]$ to be a basic sequence. If l is a natural number, then there are 2^l+1 integers whose absolute value does not exceed 2^{l-1}. On the other hand, the number of integers of the form

$$\sum_{1}^{l} \varepsilon_i 2^{i-1} d_i$$

is 2^l. It follows that there exist numbers m and k, such that

$$|m| \leqq 2^{l-1}, \quad m = 2^{k-1} d_k + \varepsilon_{k-1} 2^{k-2} d_{k-1} + \dots + \varepsilon_1 d_1, \quad k > l.$$

Now by taking l sufficiently large, we obtain a contradiction from (2.4).

Corollary. If $|d_{k+1}| \geqq |d_k| > 1$ *for all large values of k, then* $[d_1, d_2, \dots]$ *is not basic.*

In theorem 5, we shall give a sufficient condition. It is a very special one, but it shows that the d's in a basic sequence need not be bounded and that an infinity of them may be equal to one and the same odd number. Actually, from any arbitrary sequence of odd numbers we can make a basic sequence, by interpolation of sufficiently long sequences of terms ± 1 at infinitly many places.

Theorem 5. *Let* $d_1, d_2, \dots$ *bc a sequence of odd numbers. Assume that, for any positive number* A, *we have an index* l *with the property that*

$$(2\ 5) \qquad \begin{cases} |d_l| = |d_{l-1}| = 1, d_l = -d_{l-1}, \\ |d_{l-2}| + \left|\frac{d_{l-3}}{2}\right| + \left|\frac{d_{l-4}}{4}\right| + \dots + \left|\frac{d_1}{2^{l-3}}\right| \leqq 4 - 2^{3-l}A. \end{cases}$$

Then $[d_1, d_2, \dots]$ *is a basic sequence.*

Proof. Take an arbitrary integer x, choose $A > |x|$ and take l such that (2.5) holds. Consider the numbers of the form

$$(2.6) \qquad \sum_{i=1}^{l} \varepsilon_i 2^{i-1} d_i \qquad (\varepsilon_i = 0 \text{ or } 1).$$

Each residue class mod 2^l contains just one of these numbers. Let x_1 be of the form (2.6) and such that $x \equiv x_1 \pmod{2^l}$. It follows from (2.5) that $|x_1| \leqq 2^l - A$. On the other hand we have $|x| < A$, and so $|x - x_1| < 2^l$. Consequently we have $x = x_1$, and so x is of the form (2.6). Therefore, any integer can be represented by the base $\{d_1, 2d_2, 2^2 d_3, \dots\}$.

§ 3. Periodic basic sequences.

Consider a sequence of odd numbers which is, for some natural number s, periodic mod s, i. e. $d_{i+s} = d_i$ for all i.[1][2]).

If x is given, the numbers $\varepsilon_1, \dots, \varepsilon_s$ $(\varepsilon_i = 0$ or $1)$ can be determined uniquely such that in

$$(3.1) \qquad x - \sum_{i=1}^{s} \varepsilon_i 2^{i-1} d_i = 2^s x_1$$

x_1 is an integer. (See (2.3)).

This defines a mapping $x \to x_1$ of the set of integers into itself. Iterating this mapping we have $x \to x_1 \to x_2 \to \dots$. It follows from the periodicity

[1]) By theorem 2, our results can be extended immediately to sequences satisfying $d_{i+s} = d_i$ for all *sufficiently large i.*

[2]) The case $s = 1$ is not interesting; in that case theorem 3' shows that the sequence s not basic.

mod s of the sequence $[d_1, d_2, \dots]$ that x_n is uniquely determined by the condition that $\varepsilon_1, \dots, \varepsilon_{ns}$ ($\varepsilon_i = 0$ or 1) exist such that

$$(3.2) \qquad x - \sum_{i=1}^{ns} \varepsilon_i 2^{i-1} d_i = 2^{ns} x_n.$$

It follows that x can be written in the form (2.2) with $\sum \varepsilon_i < \infty$ if and only if the iterates x_n vanish for all large values of n.

The mapping $x \longrightarrow x_1$ defines a *graph*. The vertices are all the integers; two vertices a, b are connected by an oriented edge from a to b whenever we have $a \longrightarrow b$ in the mapping. Closed loops $a \longrightarrow a$ may occur, but we always remove the loop $0 \longrightarrow 0$. Clearly we have

Theorem 6. *A periodic sequence of odd integers is basic if and only if the graph of the mapping $x \longrightarrow x_1$ (defined by (3.1) is a tree.*

The root of the tree is always 0, of course. If the graph is not a tree, it still contains an infinite tree, with root 0; it consists of all integers x which can be written in the form (2.2) with $\sum \varepsilon_i < \infty$.

If $x \equiv y \pmod{2^s}$, $x \longrightarrow x_1, y \longrightarrow y_1$, we have $x - y = 2^s(x_1 - y_1)$. Hence the mapping $x \longrightarrow x_1$ is known whenever the images of the x-values $1, 2, 3, \dots, 2_s$ are known.

Lemma 2. *There exist numbers A and B, $(A < B, A \leqq 0, B \geqq 0)$, such that*

a) for $x < A$ we have $\quad x < x_1 \leqq B$
b) for $A \leqq x \leqq B$ we have $\quad A \leqq x_1 \leqq B$
c) for $x > B$ we have $\quad A \leqq x_1 < x$.

Proof. Denoting the sum in (3.1) by $u(x)$, we have $x - u(x) = 2^s x$ Putting $v(x) = u(x)/(1 - 2^s)$ we have either $x < x_1 < v(x)$ or $x = x_1 = v(x)$ or $v(x) < x_1 < x$.

For $u(x)$ we have 2^s possible values, according to the possible values for $\varepsilon_1, \dots, \varepsilon_s$. Now the numbers $A = \min\, (v(x))$, $B = \max\, (v(x))$ satisfy the conditions a, b and c. Since $0 \longrightarrow 0$, it follows from a) that $A \leqq 0$ and from c) that $B \geqq 0$.

We notice that A may be replaced by any number $A' \leqq A$ and B by any number $B' \geqq B$

Lemma 2 enables us to determine, by a finite number of operations, whether the graph is or is not a tree. Suitable numbers A and B are easily obtained; after that we consider the part of the graph whose vertices correspond to numbers x with $A \leqq x \leqq B$. By lemma 2, this part is a tree if and only if the whole graph is a tree.

Examples.

1. Consider $s = 2, d_1 = 13, d_2 = -7$. The mapping is completely described by $4t \longrightarrow t$, $4t + 1 \longrightarrow t - 3$, $4t + 2 \longrightarrow t + 4$, $4t + 3 \longrightarrow t + 1$, for all integers t

We can take $A = -4, B = 4$ and thus neglect all integers < -4 or > 4. The remaining part is a tree with root 0, for $-2 \to 3 \to 1 \to -3 \to -4 \to -1 \to 0$; $2 \to 4 \to 1 \to -3$ etc.. Hence the sequence $[13, -7, 13, -7, \dots]$ is basic.

2. Take $s = 2, d_1 = 3, d_2 = -1$. The graph turns out to contain a subtree, covering all positive, but not all negative integers. Consequently the set $\{3, -2, 3.2^2, -2^3, 3.2^4, \dots\}$ is a base for the set of natural numbers, but not for the set of all integers.

If the least possible values for $|A|$ and B are large, the application of theorem 6 can be troublesome. Then theorems 3, 4, 5 and 7 might be useful. So, for instance, theorem 7 shows that the sequence $[5, 1, -1, 1, 5, 1, -1, 1, \dots]$ is not basic, since $5 + 2 + 0\ (-2^2) + 2^3 \equiv 0 \pmod{15}$.

Theorem 7. *A necessary and sufficient condition for the odd sequence $d_1, d_2, \dots$ (with period s) to be basic, is that*

$$0 \neq \sum_{i=1}^{ns} \varepsilon_i 2^{i-1} d_i \equiv 0 \pmod{2^{ns} - 1} \tag{3.3}$$

is impossible for $n = 1, 2, 3, \dots, \varepsilon_i = 0$ or 1 $(i = 1, \dots, ns)$.

Proof. It follows from lemma 2 that the graph is a tree if and only if it contains no cyclic sub-graph. Assume (3. 3) to be true for some n and some set of ε's. Denoting the sum occurring in that formula by $(1 - 2^{ns})\, x$, we infer from (3 2) that $x = x_n$.

Since $x \neq 0$, this means the occurrence of a cycle of length n. Conversely, $x = x_n \neq 0$ means that (3. 3) is true. This proves the theorem.

It may be remarked that, in applying theorem 7 we may neglect the values of n which exceed the number of integers $\neq 0$ in the interval $A \leqq x \leqq B$. For, by lemma 2, no cycle contains numbers outside that interval, and no cycle contains the number 0.

§ 4. Sequences with the period 2.

We shall give a more detailed discussion of the case $s = 2$. Hence we consider sequences

$$[a, b, a, b, \dots], \tag{4. 1}$$

where both a and b are odd. If (4. 1) is basic, we simply say that $[a, b]$ is basic. There are infinitely many basic pairs (Theorem 9 be ow).

The property of a pair $[a, b]$ to be basic can be stated in a different form also. Let S denote the set $0, 1, 4, 5, 16, 17, 20, 21, 64, 65, \dots$ of non-negative numbers whose 4-adic representation does not contain the digits 2 and 3. Then $[a, b]$ is basic if and only if the following statement holds: *Any integer x can be represented uniquely in the form*

$$x = as_1 + 2bs_2 \qquad (s_1 \in S, s_2 \in S). \tag{4. 2}$$

So, for instance, $13s_1-14s_2$ represents all integers uniquely. (See the list at the end of this section).

We shall apply the theorems of the preceding sections to our present case. If $[a, b]$ is basic, then a and b have opposite signs, and their g. c. d. equals 1 (theorem 3). Furthermore $[b, a]$ $[-a, -b]$, $[-b, -a]$ will be basic as well (theorem 2). Theorem 4 cannot be applied; neither theorem 5 (except for $[1, -1]$ and $[-1, 1]$). Theorem 6 is of course a never failing criterion, but it reveals no general facts. Besides, its application is troublesome.

Theorem 7 gives infinitely many linear congruences none of which are satisfied by any basic pair $[a, b]$ Taking $n=1$ we find $a \not\equiv 0\,(3)$, $a+2b \not\equiv 0\,(3), b \not\equiv 0\,(3)$.

Since both a and b are odd, we infer

$$(4.3) \qquad a+b \equiv 0 \pmod 6, \qquad (a, 6)=1, (b, 6)=1.$$

There are also applications of a more general nature (heorems 8 and 9).

Theorem 8. *If either a or b is divisible by any number of the form* 2^m+1, *then* $[a, b]$ *is not basic.*

Proof. It is, of course, sufficient to show it for a. So assume that $a=(2^m+1)c$, and that $[a, b]$ is basic.

The fact that $a \not\equiv 0\,(3)$ shows that m is even, for otherwise $2^m+1 \equiv 0\,(3)$. Writing $m=2k$, we have

$$(4.4) \quad \begin{aligned} & a+2b+2^2a+2^3b+\ldots+2^{2k-2}a+2^{2k-1}b+2^{2k+1}b+2^{2k+3}b+\ldots+2^{4k-1}b= \\ & =a(1+2^2+2^4+\ldots+2^{2k-2})+2b(1+2^2+2^4+\ldots+2^{4k-2})= \\ & =\tfrac{1}{3}a(2^{2k}-1)+\tfrac{2}{3}b(2^{4k}-1)=\tfrac{1}{3}(c+2b)(2^{4k}-1) \end{aligned}$$

By (4. 3) we have $(2^{2k}+1)c+b \equiv 0\,(3)$, and so $c+2b \equiv 0\,(3)$. It follows that the expression (4. 4) is divisible by $2^{4k}-1$. Now theorem 7, with $s=2, n=2k$ shows that $[a, b]$ is not basic.

Theorem 9. *The pair* $[2^{2k+1}-1, -1]$ *is basic* $(k=0, 1, 2, \ldots)$.

Proof. Assume (3.3) to be possible for a certain n; in the present case this means

$$(4.5) \quad \begin{gathered} (2\,4^k-1)(\delta_0+4\delta_1+4^2\delta_2+\ldots+4^{n-1}\delta_{n-1})-2(\eta_0+4\eta_1+\ldots+4^{n-1}\eta_{n-1}) \\ \equiv 0 \pmod{4^n-1} \end{gathered}$$

for a special set of numbers δ_i and η_i, each one of them being either 0 or 1, but at least one of them being 1. For $i<0$ and $i \geqq n$ we define δ_i by $\delta_i=\delta_j$ where $j \equiv i$ (n) and $0 \leqq j<n$ Now we can infer from (4 5) that the number

$$(4.6) \quad \begin{gathered} -(\delta_0+4\delta_1+\ldots+4^{n-1}\delta_{n-1})+ \\ +2\{(\delta_{-k}-\eta_0)+4(\delta_{-k+1}-\eta_1)+\ldots+4^{n-1}(\delta_{-k+n-1}-\eta_{n-1})\} \end{gathered}$$

is a multiple of 4^n-1. The absolute value of (4. 6) is less than 4^n-1; consequently it is zero. It easily follows that all δ's and η's are zero, which contradicts our assumption.

Necessary conditions for $[a, b]$ to be basic can also be obtained by considering the ratio $t=-a/b$. By T we denote the set of t's arising from basic pairs. We notice that $t\in T$ implies that $t>0$ and $t^{-1}\in T$.

We can find infinitely many intervals which contain no points of T. Consider a basic pair $[a, b]$ with $a>-b>0$, and take $x=-1$ in (4 2). It follows that t can be written in the form $(s_1+a^{-1})/2s_2$, $s_1\in S, s_2\in S$. It is easily verified that $(s_1+a^{-1})/2s_2$ is contained in at least one of the closed intervals ($n=0, 1, 2, \ldots,$ $k=0, 1, 2, \ldots$)

$$\left(\frac{4^{n+k}}{\frac{2}{3}(4^{n+1}-1)}, \frac{\frac{1}{3}(4^{n+k+1}-1)+a^{-1}}{2\,4^n}\right)$$

unless $a=t=s_1=s_2=1$. It follows that the open intervals

$$\left(1, \frac{3}{2}\right), \left(3, 6\right), \left(11, 24\right), \ldots, \left(\frac{2}{3}\,4^{k+1}+\frac{1}{3}, 6.4^k\right), \ldots$$

are all free from points of T.

It is not difficult to obtain more intervals, but their total measure seems to be relatively small.

We conclude this section with a list of all basic pairs $[a, b]$, as far as $100\geqq a>-b>0$. They are:

$[1,-1]$, $[7,-1]$, $[31,-1]$, $[37,-1]$, $[13,-7]$, $[43,-7]$, $[73,-7]$, $[23,-11]$, $[89,-11]$, $[31,-13]$, $[31,-19]$, $[49,-31]$, $[61,-31]$, $[67,-31]$, $[73,-31]$, $[77,-41]$, $[83,-41]$, $[71,-47]$, $[77,-47]$, $[97,-49]$.

§ 5. Generalizations.

A simple generalization of the notion of a base is obtained as follows. Let A be a finite set of h natural numbers $a_1, \ldots, a_h$, and assume $0\in A$. The set $\{b_1, b_2, \ldots\}$ will now be called an A-base, whenever any integer x can be written in the form

$$(5.\ 1) \qquad x=\sum_{i=1}^{\infty}\varepsilon_i b_i. \qquad \left(\varepsilon_i\in A, \sum|\varepsilon_i|<\infty\right).$$

The example $h=3, A=\{-1, 0, 1\}, b_i=3^{i-1}$ is well-known from BACHET's weight problem.

An A-base will be called *simple* if it can be rearranged into the form $\{d_1, hd_2, h^2d_3, \ldots\}$. It is easily seen that, in that case, the numbers $a_1d_1, \ldots, a_hd_1$ form a complete residue system mod h. Hence $a_1, \ldots, a_h$ form a complete residue system, and $(d_1, h) = 1$. The argument can be repeated, which leads to $(d_2, h) = (d_3, h) = \ldots = 1$.

A large part of the contents of the preceding sections can be extended to simple A-bases. (The expansions (2. 2), theorem 2, the second part of theorem 3, theorem 4 and the whole of § 3).

We do not yet know which sets A have the property that there exists any simple A-base. A necessary condition is, as we saw above, that $a_1, \ldots, a_h$ form a complete set of residues mod h. A further trivial necessary condition is, that no prime divides all numbers of A.

If A consists of h consecutive numbers (including 0), then we can show, by straightforward extension of theorem 5, that infinitely many A-bases exist. Actually, any sequence $\{\pm 1, \pm h, \pm h^2, \ldots\}$ is an A-base, whenever both $+1$ and -1 occur infinitly often. The latter restriction is superfluous if A contains elements of either sign. Furthermore it is clear that periodic basic sequences exist also.

The next problem is, which A's have the property that there exists any non-simple A-base. Such A's exist indeed: if we take $h = 4, A = \{0, 1, 4, 5,\}$, then $\{1, 2, -2^4, -2^5, 2^8, 2^9, -2^{12}, -2^{13}, \ldots\}$ is a non-simple A-base.

On the other hand, it is easily proved that every A-base is simple, whenever A consists of h consecutive numbers $(0 \in A)$, where h is a prime. The proof can be given by direct extension of the proof of lemma 1.

The problem as to the existence and structure of non-simple A-bases is related to a few conjectures on abelian groups, which we state below.

Considering addition as the group operation, an abelian group G is said to be the direct sum of the sub-sets $S_1, \ldots, S_n$, if every element $g \in G$ can be uniquely represented in the form $g = s_1 + \ldots + s_n, s_i \in S_i$. We write $G = S_1 + \ldots + S_n$. If H is a sub-group of G, a sub-set $S \subset G$ is said to be periodic mod H, whenever $s \in S$, $h \in H$ imply $s + h \in S$.

Conjecture 1. *Let G be a finite abelian group of order >1, and assume $G = S_1 + S_2$. Then either S_1 or S_2 is periodic mod some sub-group of order >1.*

If G is infinite, then neither S_1 nor S_2 need to be periodic (see (4. 2), where neither aS nor $2bS$ are periodic) If however S_1 is finite, and G is the group of all integers, then S_2 is periodic[8]).

The following conjecture is a consequence of conjecture 1:

Conjecture 2. *Let R be the set of all integers. Let p be a prime: Let S_1 be a set of p integers, 0 being one of them, and assume that the integers of S_1 have no common factor. Finally assume $R = S_1 + S_2$, and*

[8]) See a problem, suggested by the author: *Matematikai Lapok* 1 (1950), p. 153

$0 \in S_2$. *Then* S_2 *is the set of all multiples of* p, *and* S_1 *is a complete set of residues mod* p.

This can be derived from conjecture 1 as follows. As it was remarked before, S_2 is periodic; let m be its exact period. If M denotes the group of residue classes mod m, then $R = S_1 + S_2$ furnishes a dissection $M = S_1^* + S_2^*$, where S_i^* consists of the residue classes determined by the elements of S_i. S_2^* can not be periodic mod any proper sub-group of M, for this would imply that the period of S_2 is less than m. Hence S_1^* is periodic mod H, where H is a group of order >1. Clearly the number of elements of S_1^* is a multiple of the order of H; it follows that the latter number equals p.

The group M has only one sub-group of order p; its elements are $\equiv 0$ (mod m/p). The elements of S_1 were assumed to have no common factor, whence $m = p$. It follows that S_2^* consists of but one element: this is the residue class $\equiv 0$ (mod p) This implies that S_2 is the set of all p-tuples, and S_1 is a complete residue system mod p.

The conditions a: "p is a prime" and b: "the integers of S_1 have no common factors", should not be omitted. This is demonstrated by the following examples.

a) Take $S_1 = \{0, 1, 4, 5\}$, S_2 the set of all numbers $\equiv 0$ or $\equiv 2$ (mod 8). Then $R = S_1 + S_2$, and S_2 does not consist of all 4-tuples.

b) Take $p = 3, S_1 = \{0, 2, 4\}, S_2$ the set of all numbers $\equiv 0$ or $\equiv 1$ (mod 6). Again $R = S_1 + S_2$, and S_2 does not consist of all 3-tuples.

It is possible to give a proof, independent of conjecture 1, of the second part of conjecture 2, namely that S_1 is a complete set of residues mod p. Namely, let m be the period of S_2, and let $M = S_1^* + S_2^*$ as above. Let $a_1, a_2, \ldots, a_p$ and $b_1, \ldots, b_{m/p}$ be non-negative representatives of the residue classes contained in S_1^* and S_2^*, repectively. Put

$$f(x) = \sum_{i=1}^{p} x^{a_i}, \; g(x) = \sum_{i=1}^{m/p} x^{b_i}.$$

Then we have, operating in the ring of polynomials with integer coefficients,

$$f(x)\, g(x) \equiv 1 + x + x^2 + \ldots + x^{m-1} \qquad (\text{mod } x^m - 1)$$

If the h-th cyclotomic polynomial is denoted by $K_h(x)$, we infer that $f(x)\, g(x)$ is divisible by $\prod_{d/m,\, d>1} K_d(x)$. We have $f(1) = p$, $g(1) = m/p$, $\prod_{a/m,\, d>1} K_d(1) = m$; $K_d(1) = q$ if d is a power of a prime q, and $K_d(1) = 1$ otherwise. The polynomials $K_d(x)$ being irreducible, it follows that $f(x)$ is, for some λ, divisible by $K_{p^\lambda}(x) = 1 + x^{p^{\lambda-1}} + x^{2p^{\lambda-1}} + \ldots + x^{(p-1)\, p^{\lambda-1}}$

If we reduce $f(x)$ (mod $x^{p^\lambda} - 1$) to a polynomial $f_1(x)$ of degree $< p^\lambda$, then $f_1(x)$ has non-negative coefficients, whose sum equals p. Whereas $f_1(x) \equiv 0$ (mod $K_{p^\lambda}(x)$), we infer that the coefficient of $x^{kp^{\lambda-1}}$ $(k = 1, 2, \ldots, p-1)$ is the same as the coefficient of x^0, which is 1. The sum of the coefficients of $f_1(x)$ being p, we find that $f_1(x)=K_{p^\lambda}(x)$. If $\lambda \geqq 1$, this means that all numbers of S_1 are $\equiv 0 \pmod{p}$, which was excluded beforehand. Consequently $f_1(x)=1+x+\ldots+x^{p-1}$, whence it follows that S_1 is a complete residue system mod p

It seems to be difficult to prove the first part of conjecture 2 along the same lines. It would be accomplished by showing that $f(x)$ is not divisible by any cyclotomic polynomial different from $K_p(x)$ (then it would follow that $g(x)\equiv 0$ (mod $(x^m-1)/K_p'x)$) etc) This is trivial for $p=2$ and still true[4]) for $p=3$, but it fails for $p=5$: the polynomial $1+x^2+x^3+$ $+x^4+x^6$ is divisible by $K_6(x)$ Nevertheless the dissection $R=\{0,2,3,4,6\}+$ $+S_5$, $0\in S_5$, implies that S_5 consists of all multiples of 5

If conjecture 2 is true, then we have immediately: *if the number of elements of A is a prime, then every A-base is simple.*

The author does not know whether the following conjecture, which includes conjecture 1 as a special case, is a consequence of conjecture 1.

Conjecture 3. *Let G be a finite abelian group of order >1, and $G=S_1+\ldots+S_n$, then at least one of the S's is periodic mod some subgroup of order >1.*

A special case was proved by G. HAJÓS[5]), who assumed that each S_i consists of the multiples $0, A_i, 2A_i, 3A_i, \ldots, a_iA_i$ of a group-element A_i.

A still more difficult problem is to find all dissections of the set R of all integers into a finite or an infinite number of components S. For simplicity it can be assumed that 0 belongs to all components S. If the number of components is ∞, then $R=S_1+S_2+\ldots$ has to be interpreted as follows: any number x can be represented uniquely in the form $x=\sum_1^\infty{}' s_i$ $(s_i\in S)$, where all but a finite number of the s_i equal zero.

At present we do not attempt any speculations as to the structure of these dissections.

(Received August 21, 1950.)

[4]) This can be derived from the fact that $1+x^a+x^b=0$, $(a,b)=1$, $|x|=1$ imply that x is a primitive third root of unity.

[5]) G HAJÓS: Über einfache und mehrfache Bedeckung des n-dimensionalen Raumes mit einem Würfelgitter, *Math. Z.* 47 (1942), 427—467.