Chapter XII

SOME PROBLEMS OF THE ADDITIVE THEORY OF NUMBERS

§ 1. Partitio numerorum. Leibniz and Bernoulli and later on Euler were the first to consider the problem of establishing the number g_n of all possible representations of an arbitrary natural number n as the sum of non-increasing natural numbers. This problem is known under the name *partitio numerorum*.

Here are the initial ten values of the function g_n: $g_1 = 1$, $g_2 = 2$, $g_3 = 3$, $g_4 = 5$, $g_5 = 7$, $g_6 = 11$, $g_7 = 15$, $g_8 = 22$, $g_9 = 30$, $g_{10} = 42$.

Mac Mahon has found that $g_{100} = 1905692292$ and $g_{200} = 3972999029388$.

It can be proved that the numbers g_n are the coefficients of the expansion into a power series of the function

$$\prod_{n=1}^{\infty} \frac{1}{1-x^n} = 1 + \sum_{n=1}^{\infty} g_n x^n \quad \text{for} \quad |x| < 1.$$

Let h_n be the number of different representations of a number n as the sum of increasing natural numbers. It is easy to prove that, for $|x| < 1$,

$$\prod_{n=1}^{\infty} (1+x^n) = 1 + \sum_{n=1}^{\infty} h_n x^n.$$

The numbers g_n $(n = 1, 2, \ldots)$ satisfy the inductive identity

$$n g_n = \sigma(n) + g_1 \sigma(n-1) + g_2 \sigma(n-2) + \ldots + g_{n-1} \sigma(1),$$

which may serve as a rule for finding g_n's (cf. Vahlen [1]).

Here are the initial ten values of the function h_n: $h_1 = 1$, $h_2 = 1$, $h_3 = 2$, $h_4 = 2$, $h_5 = 3$, $h_6 = 4$, $h_7 = 5$, $h_8 = 6$, $h_9 = 8$, $h_{10} = 10$.

Denote by k_n the number of all possible decompositions of a natural number n into the sum of natural numbers, where two decompositions are considered as different also if they differ only in the order of the summands.

Easy induction shows that

$$k_n = 2^{n-1} \quad \text{for any } n = 1, 2, \ldots$$

Thus, in particular, the number 4 has eight different decompositions into the sum of natural numbers:

$$4 = 3+1 = 1+3 = 2+2 = 2+1+1 = 1+2+1 = 1+1+2 = 1+1+1+1.$$

Finally, let l_n denote the number of all possible decompositions of a natural number n into the sum of non-decreasing odd natural numbers. Then, for $|x| < 1$, we have

$$\prod_{n=1}^{\infty} \frac{1}{1-x^{2n-1}} = 1 + \sum_{n=1}^{\infty} l_n x^n.$$

It is worth-while to mention that it can be proved that the equality $l_n = h_n$ holds for any $n = 1, 2, \ldots$

Let q_n be the function which assigns to a natural number n the number of partitions of the set of n elements into non-void disjoint subset, two partitions that differ only in the order of the parts being regarded as identical.

The initial values of this function are $q_1 = 1$, $q_2 = 2$, $q_3 = 5$, $q_4 = 15$, $q_5 = 52$.

We have the following inductive formula for q_n (Ore [1]):

$$q_{n+1} = 1 + \sum_{k=1}^{n} \binom{n}{k} q_k.$$

We also have (Birkhoff [1], p. 17, and Williams [1])

$$e^{e^x - 1} = \sum q_n x^n / n!.$$

The number of different representations of an integer as the sum reduced with respect to the modulus m of the numbers of the sequence $1, 2, \ldots, m-1$ has also been considered. M. A. Stern [1] has proved that, if p is an odd prime, then any residue to p has precisely $(2^{p-1}-1)/p$ such representations, where the summands are $1, 2, \ldots, p-1$.

For example, if $p = 5$,

$$0 \equiv 1+4 \equiv 2+3 \equiv 1+2+3+4 \pmod 5,$$
$$1 \equiv 1 \equiv 2+4 \equiv 1+2+3 \pmod 5,$$
$$2 \equiv 2 \equiv 3+4 \equiv 1+2+4 \pmod 5,$$
$$3 \equiv 3 \equiv 1+2 \equiv 1+3+4 \pmod 5,$$
$$4 \equiv 4 \equiv 1+3 \equiv 2+3+4 \pmod 5.$$

§ 2. Representations as sums of n non-negative summands. We now prove that if n and k are two given natural numbers, then the number $F_{n,k}$ of all possible representations of the number k as the sum of n non-negative integers, where two representations that differ in the order of the summands are also regarded as different, is $\binom{n+k-1}{k}$.

In fact, we have $F_{1,k} = 1 = \binom{k}{k}$. Suppose that for a natural number n the formula $F_{n,k} = \binom{n+k-1}{k}$ is valid for any $k = 1, 2, \ldots$ Then it is easy to see that

$$F_{n+1,k} = F_{n,k}+F_{n,k-1}+F_{n,k-2}+\ldots+F_{n,1}+1$$
$$= \binom{n+k-1}{k}+\binom{n+k-2}{k-1}+\binom{n+k-3}{k-2}+\ldots+\binom{n}{1}+1.$$

For any two natural numbers n and k the identity

$$\binom{n+k}{k} = \binom{n+k-1}{k}+\binom{n+k-1}{k-1}$$

holds. This implies that

$$\binom{n+k}{k} = \binom{n+k-1}{k}+\binom{n+k-2}{k-1}+\ldots+\binom{n}{1}+\binom{n}{0}.$$

Consequently,

$$F_{n+1,k} = \binom{n+k}{k},$$

which shows that the formula $F_{n,k} = \binom{n+k-1}{k}$ for $k = 1, 2, \ldots$ is true for any n.

Another proof of the same formula is this. To each decomposition $k = a_1+a_2+\ldots+a_n$ of a natural number k into the sum of n non-negative integers we relate the sequence of the numbers $l_i = a_1+a_2+\ldots+a_i+i$, where $i = 1, 2, \ldots, n-1$. It is clear that this sequence consists of increasing natural numbers each of which is $\leqslant n+k-1$. As is known the number of such sequences is equal to $\binom{n+k-1}{n-1} = \binom{n+k-1}{k}$.

T. Skolem [3] has discussed the problem which are the natural numbers n such that the set of the numbers $1, 2, \ldots, 2n$ can be divided into n pairs (a_i, b_i) $(i = 1, 2, \ldots, n)$ in such a way that $b_i - a_i = i$ for any $i = 1, 2, \ldots, n$.

If a number n has this property, then

$$\sum_{i=1}^{n} b_i - \sum_{i=1}^{n} a_i = 1+2+\ldots+n = n(n+1)/2.$$

But, since the numbers $a_1, b_1, a_2, b_2, \ldots, a_n, b_n$ are equal to the numbers $1, 2, \ldots, 2n$ in a certain order, we see that $\sum_{i=1}^{n} a_i + \sum_{i=1}^{n} b_i = 1+2+\ldots+2n = n(2n+1)$. Hence $\sum_{i=1}^{n} b_i = \frac{1}{4}n(5n+3)$, which is easily proved not to be an integer provided n is congruent to 2 or 3 (mod 4). Conversely, as proved by T. Skolem in the paper referred to above (cf. O'Keefe [1]), if n is congruent to 0 or to 1 (mod 4), then the partition in question is always possible. For example, if $n = 4$, then the pairs of the partition are $(6, 7)$, $(1, 3)$, $(2, 5)$, $(4, 8)$; if $n = 5$, the pairs of the partition are $(2, 3)$, $(6, 8)$, $(7, 10)$, $(1, 5)$, $(4, 9)$.

§ 3. Magic squares. A square array of the integers $1, 2, .., n^2$ such that the sums of the numbers in each row, each column and each diagonal are the same is called a *magic square* of degree n. It is easy to calculate that the common value of all these sums is $\frac{1}{2}n(n^2+1)$. The case of $n = 1$ is trivial. For $n = 2$ it is easy to prove that no magic square exists. For $n = 3$ an example of a magic square is

8	1	6
3	5	7
4	9	2

If $n = 4$, examples of magic squares are the following:

16	3	2	13
5	10	11	8
9	6	7	12
4	15	14	1

10	5	11	8
3	16	2	13
6	9	7	12
15	4	14	1

1	15	10	8
14	4	5	11
7	9	16	2
12	6	3	13

4	10	15	5
7	13	12	2
14	8	1	11
9	3	6	16

14	1	12	7
11	8	13	2
5	10	3	16
4	15	6	2

2	13	8	11
12	7	14	1
15	4	9	6
5	10	3	16

Here are the examples for $n = 5, 6, 7$

17	24	1	8	15
23	5	7	14	16
4	6	13	20	22
10	12	19	21	3
11	8	25	2	9

1	35	4	33	32	6
25	11	9	28	8	30
24	14	18	16	17	22
13	23	19	21	20	15
12	26	27	10	29	7
36	2	34	3	5	31

30	39	48	1	10	19	28
38	47	7	9	18	27	29
46	6	8	17	26	35	37
5	14	16	25	34	36	45
13	15	24	33	42	44	4
21	23	32	41	43	3	12
22	31	40	49	2	11	20

There exists precisely one magic square for $n = 3$, provided we identify the magic squares obtained from a given one by rotation or reflexion. According to Frenicle, however, there exist 880 magic squares for $n = 4$, and according to Mac Mahon there are some 60000 magic squares for $n = 5$. It is proved that there exist magic squares for any $n \geqslant 3$ (cf. L. Bieberbach [1]).

The proof of the existence of magic squares for an arbitrarily large n which we are going to present here is due to A. Mąkowski. First we show how, having two magic squares Q_n and Q_m of degree n and m respectively, we can obtain a magic square Q_{nm} of degree nm. This can be done simply by substituting the square Q_n for each number i of the square Q_m

provided the number $n^2(i-1)$ is added to each number of the square Q_n. It is easy to see that the square thus obtained is indeed a magic square of degree mn, the sums of the numbers of each column, each row and each diagonal of the square Q_{nm} being equal to $\frac{1}{2}mn(n^2+1)+\frac{1}{2}n^3m(m^2-1)$.

This provides a method of constructing magic squares of degree 3^k, $k = 1, 2, \ldots$, from the magic square of degree 3.

A magic square of an odd degree is called *perfect* if the sum of any two numbers of the square that are in symmetric positions with respect to the number in the middle of the square is equal to double the number in the middle. Any magic square of degree 3 is perfect (the number in the middle being equal to 5). However, there are magic squares of degree five that are not perfect (for example, such is the magic square of degree 5 due to Stiffel and presented below). Here is an example of a perfect magic square of degree 5.

11	4	17	10	23
24	12	5	18	6
7	25	13	1	19
20	8	21	14	2
3	16	9	22	15

The magic square of degree seven presented above is perfect.

There exist magic squares that consist of different n^2 integers but not necessarily of the integers $1, 2, \ldots, n^2$. For example,

18	2	13
6	11	16
9	20	4

43	1	67
61	37	13
7	73	31

17	13	2	8
1	9	16	14
18	12	3	7
4	6	19	1

Another more general example is this:

$s-3$	1	$s-6$	8
$s-7$	9	$s-4$	2
6	$s-8$	3	$s-1$
4	$s-2$	7	$s-9$

where $s > 18$.

Magic squares (in the wider sense) have been found consisting of different prime numbers. For example,

569	59	449
239	359	479
269	659	149

17	317	397	67
307	157	107	227
127	277	257	137
347	47	37	367

(cf. Moessner [2] and [3]).

As has been noticed by A. Mąkowski, if the terms of the arithmetical progression $a+b$, $2a+b$, ..., n^2a+b are prime numbers, then replacing the number i by the number $ia+b$ in a magic square consisting of the numbers $1, 2, \ldots, n^2$ we obtain a magic square (in the wider sense) that consists of prime numbers.

As we have already learned, conjecture implies the existence of numbers x such that any of the numbers $x+1$, $2x+1$, ..., n^2x+1 is prime. Therefore conjecture implies the existence of magic squares of degree n for any $n > 2$ consisting of prime numbers.

A. Moessner has constructed a magic square of degree 8 that consists of triangular numbers $t_0, \ldots, t_{63}$. The square is such that the sum of the numbers in each row, each column and each diagonal is the triangular number t_{104}. (Cf. Moessner [1].)

A magic square (in the wider sense) is called *almost magic* if it is formed of the numbers s, $s+1$, ..., $s+n^2$. It is clear that such a square will become a magic square (in the narrower sense) if from any of its numbers the number $s-1$ is subtracted. As announced by L. Bieberbach [1], in the year 1544 Michael Stieffel considered almost magic squares

which after removing the first and the last row and the first and the last column remain almost magic squares. It can be proved that there exist such squares with an arbitrary > 4 number of rows.

Here is an example of such a square due to Stieffel

5	6	23	24	7
22	12	17	10	4
18	11	13	15	8
1	16	9	14	25
19	20	3	2	21

This is a magic square (in the narrower sense) formed of the numbers $1, 2, \ldots, 25$. After removing the first and the last row and the first and the last column of the square we obtain an almost magic square formed of the numbers $9, 10, \ldots, 17$.

The squares formed of natural numbers such that the products of the numbers of each row, each column and each diagonal are the same have also be considered. Such are for instance the squares (cf. Goodstein [1])

2	256	8
64	16	4
32	1	128

6	36	8
16	12	9
18	4	24

24	81	24
36	36	36
54	16	54

The bibliography concerning magic squares up to the beginning of the 20th century is to be found in P. Bachmann [1]. Many methods of constructions of magic squares are presented in Postnikov [1].

§ 4. Schur's theorem and its corollaries.

LEMMA. *If k is a natural number, $N = [ek!]$, if $a_0 < a_1 < a_2 < \ldots < a_N$ is a sequence of integers and if the set of the differences $a_j - a_i$, where $0 \leqslant i < j \leqslant N$, is divided into k disjoint classes, then at least one of the classes contains the differences $a_m - a_l$, $a_n - a_l$, $a_n - a_m$ for some l, m, n such that $0 \leqslant l < m < n \leqslant N$.*

Proof. Suppose to the contrary that for a natural number k the lemma is false. Let K_1 denote the class that contains the maximal possible number of differences of the form $a_j - a_0$, where $0 < j \leqslant N$, and let $a_{j_1} - a_0$, $a_{j_2} - a_0$, ..., $a_{j_{k_1}} - a_0$ be the members of the class K_1 ordered according to their magnitude. We then have $N \leqslant k_1 k$.

By assumption, the $k_1 - 1$ differences

$$a_{j_2} - a_{j_1}, \quad a_{j_3} - a_{j_1}, \quad \ldots, \quad a_{j_{k_1}} - a_{j_1} \tag{1}$$

do not belong to the class K_1. Consequently, they must belong to the remaining $k_1 - 1$ classes. Let K_2 denote the one that contains the maximal number k_2 of the differences of (1). Suppose that K_2 contains the differences

$$a_{j_\alpha} - a_{j_1}, \quad a_{j_\beta} - a_{j_1}, \quad a_{j_\gamma} - a_{j_1}, \quad \ldots, \tag{2}$$

where $\alpha < \beta < \gamma < \ldots$ It is clear that $k_1 - 1 \leqslant k_2(k-1)$.

If the first number of (2) is subtracted from any of the remaining $k_2 - 1$ numbers, then we obtain the differences

$$a_{j_\beta} - a_{j_\alpha}, \quad a_{j_\gamma} - a_{j_\alpha}, \quad \ldots, \tag{3}$$

which can belong neither to the class K_1 nor to the class K_2. Consequently, they must belong to the remaining $k-2$ classes. Let K_3 denote the class that contains the maximal number k_3 of the numbers of (3). We then have $k_2 - 1 \leqslant k_3(k-2)$. Continuing in this way we ultimately obtain a sequence of natural numbers $k_1, k_2, \ldots, k_s$, where $s \leqslant k$ and

$$k_i - 1 \leqslant k_{i+1}(k-i) \quad \text{for} \quad i = 1, 2, \ldots, s-1, \tag{4}$$

with $k_s = 1$, since, if $k_s > 1$, the procedure described above applied once more would produce the number k_{s+1}. By (4), we infer that

$$\frac{k_i}{(k-i)!} \leqslant \frac{k_{i+1}}{(k-i-1)!} + \frac{1}{(k-i)!}, \qquad i = 1, 2, \ldots, s-1,$$

whence, adding the inequalites, we obtain

$$\frac{k_1}{(k-1)!} \leqslant \frac{1}{(k-1)!} + \frac{1}{(k-2)!} + \ldots + \frac{1}{(k-s)!} < e - \frac{1}{k!}.$$

Hence $N \leqslant k_1 k < ek! - 1$, contrary to the definition of N. The lemma is thus proved.

THEOREM 1 (I. SCHUR [1]). *Suppose that for a natural number k the numbers $1, 2, \ldots, [ek!]$ are divided into k classes. Then at least one of the classes contains two numbers of the sequence and their difference.*

[1] Schur [1], cf. also Bachmann [3].

Proof. If we set $a_i = i$, $i = 1, 2, \ldots, [ek!]$, in the lemma and note that among the numbers $1, 2, \ldots, [ek!]$ all the differences $a_j - a_i$ with $0 \leqslant i \leqslant j \leqslant [ek!]$ appear and, moreover, $a_n - a_m = (a_n - a_1) - (a_m - a_1)$, theorem 1 follows at once.

In connection with theorem 1 one may ask the following question. Given a natural number k, which is the least number $N = N(k)$ which has the same property as the number $[ek!]$, i.e. is such that, if the set of the numbers $1, 2, \ldots, N$ is divided into k classes, then at least one of the classes contains two numbers of the set $1, 2, \ldots, N$ together with their difference. Theorem 1 states that $N(k) \leqslant [ek!]$. Therefore $N(1) \leqslant 2$, $N(2) \leqslant 5$, $N(3) \leqslant 16$. On the other hand, clearly, $N(1) \neq 1$, so $N(1) = 2$. Since the numbers $1, 2, 3, 4$ can be divided into two classes, $1, 4$ and $2, 3$, neither of which contains two numbers together with their difference, we see that $N(2) > 4$; so since $N(2) \leqslant 5$, we have $N(2) = 5$. As proved by I. Schur, $N(k+1) \geqslant 3N(k) - 1$ (cf. exercise 1, below). Hence $N(k) \geqslant (3^k + 1)/2$, the equality being possible only in the case of $k = 1, 2, 3$.

THEOREM 2. *Let $0 < a_0 < a_1 < \ldots < a_N$ be a sequence of integers with $N = [ek!]$. If the sequence contains no arithmetical progression of at least three terms, then any partition of the set $1, 2, \ldots, a_N$ into k classes has the following property: at least one of the classes contains two different numbers and their sum.*

The proof is easily deduced from the lemma and from the following three obvious remarks:

1) among the numbers $1, 2, \ldots, a_N$ all the differences $a_j - a_i$ with $0 \leqslant i < j \leqslant N$ are contained,

2) $a_n - a_l = (a_n - a_m) + (a_m - a_l)$,

3) $a_n - a_m \neq a_m - a_l$, since the numbers a_l, a_m, a_n are not in an arithmetical progression.

COROLLARY 1. *If k is a natural number, $n \geqslant 2^{[ek!]}$, and the set $1, 2, \ldots, n$ is divided into k classes, then at least one of the classes contains two different numbers and their sum.*

To prove the corollary it is sufficient to set $a_i = 2^i$, $i = 0, 1, 2, \ldots, [ek!]$ in theorem 2 and to note that the sequence 2^i $(i = 0, 1, 2, \ldots)$ does not contain any arithmetical progression that has three terms.

As an immediate consequence of corollary 1 we have

COROLLARY 2. *If the set of all natural numbers is divided into finitely many classes, then at least one of the classes contains two different natural numbers and their sum* (cf. Rado [1]).

In connection with theorem 2 the following question arises. Given a natural number k, which is the least natural number $n = n(k)$ with the following property: if the numbers $1, 2, \ldots, n$ are divided into k

classes, then at least one class contains two different numbers together with their sum.

Clearly, we have $n(1)=3$. It can be proved that $n(2)=9$. The inequality $n(2)\geqslant 9$ follows from the fact that the set of the numbers $1,2,\ldots,8$ can be divided into the classes $A=\{1,2,4,8\}$ and $B=\{3,5,6,7\}$ such that neither of them contains the sum of any two numbers contained in it. Consequently, in order to prove that indeed $n(2)=9$, it is sufficient to prove that if the set of the numbers $1,2,\ldots,9$ is divided into two classes, then at least one of them is such that it contains two different numbers and their sum. The proof of this fact is presented in detail in my book in Polish (Sierpiński [25], pp. 427-428).

As regards the number $n(3)$, we mention here a remark due to T. Kaczmarczyk, namely that $n(3)\geqslant 24$. The argument follows from the fact that the natural numbers $1,2,\ldots,23$ can be divided into three classes A,B,C such that none of the classes contains the sum of any two elements contained in it. In fact, we set $A=\{1,2,4,8,11,22\}$, $B=\{3,5,6,7,19,21,23\}$, $C=\{9,10,12,13,14,15,16,17,18,20\}$. On the other hand G. W. Walker [1] has announced (without a proof) that $n(3)=24$, $n(4)=67$, $n(5)=197$. He also formulated the inequality $2n(k)<n(k+1)\leqslant 3n(k)$ for any $k=1,2,\ldots$

Another problem connected with this topic is this: Given a natural number N, which is the maximal number $r=r(N)$ such that there exists a sequence $a_1,a_2,\ldots,a_r$ consisting of the natural numbers $\leqslant N$ and containing no arithmetical progression that has three terms. (The sequence $a_1,a_2,\ldots,a_r$ is called A-sequence belonging to N.) It is easy to prove that $r(1)=1$, $r(2)=r(3)=2$, $r(4)=3$, $r(5)=r(6)=r(7)=4$. P. Erdös and P. Turán [1] have proved that $r(8)=4$, $r(9)=r(10)=5$, $r(11)=r(12)=6$, $r(13)=7$, $r(14)=r(15)=r(16)=r(17)=r(18)=r(19)=8$, $r(21)=r(22)=r(23)=9$ [1] and quoted the conjecture of G. Szekeres that the equality $r\left(\frac{1}{2}(3^k+1)\right)=2^k$ holds for any $k=0,1,2,\ldots$ The conjecture, however, turned out to be false; as is shown by F. Behrend [1], $r(N)>N^{1-c/\sqrt{\log N}}$, where c is a constant (cf. Salem and Spencer [1], [2], Moser [3]).

On the other hand, K. F. Roth [1] has proved that

$$\overline{\lim_{n\to\infty}}\frac{r(n)}{n}\log\log n\to\infty.$$

EXERCISES. **1.** Prove the theorem of I. Schur stating that $N(k+1)>3N(k)-1$.

Proof. It follows from the definition of $N(k)$ that the set of the numbers $1,2,\ldots,N(k)-1$ can be divided into k classes in such a way that none of the classes

[1] P. Erdös and P. Turán have stated that $r(20)=8$ this, however, is not true, because, as shown by A. Mąkowski [2], $r(20)=9$.

contains the difference of any two numbers contained in it. Let $K_i=\{x_1^{(i)},x_2^{(i)},\ldots,x_{s_i}^{(i)}\}$ $(i=1,2,\ldots,k)$. Let

$$L_i=\{3x_1^{(1)}-1,\ 3x_1^{(i)}-1,\ 3x_2^{(i)},\ \ldots,\ 3x_{s_i}^{(i)},\ 1,\ 3x_{s_i}^{(i)}\},\quad i=1,2,\ldots,k,$$
$$L_{k+1}=\{1,\ 4,\ 7,\ \ldots,\ 3N(k)-2\}.$$

It is easy to verify that none of the classes L_i $(i=1,2,\ldots,k+1)$ contains the difference of any two numbers contained in it and all the classes L_i $(i=1,2,\ldots,k+1)$ together contain all the natural numbers $1,2,\ldots,3N(k)-2$. It follows from the definition of $N(k+1)$ that $N(k+1)>3N(k)-2$, whence $N(k+1)\geqslant 3N(k)-1$.

2. Prove that $n(k+1)\geqslant 2n(k)+1$.

Proof. It follows from the definition of $n(k)$ that the numbers $1,2,\ldots,n(k)-1$ can be divided into k classes in such a way that none of them contains the sum of any two numbers contained in it. To this classes we add another class consisting of the numbers $n(k),n(k)+1,n(k)+2,\ldots,2n(k)$. Thus we obtain a partition of the set of the numbers $1,2,\ldots,2n(k)$ into $k+1$ classes which has an analogous property. It follows from the definition of the number $n(k+1)$ that $n(k+1)\geqslant 2n(k)+1$.

Remark. A. Mąkowski [3] has proved a stronger inequality, namely $n(k+1)\geqslant 2n(k)+\frac{1}{2}k(k+1)+1$.

3. Prove that $r(m+n)\leqslant r(m)+r(n)$ (Erdös and Turán).

The proof follows from the remark that, if $a_1<a_2<\ldots<a_r$ is an A-sequence that belongs to the number N, then $a_1-k,\ldots,a_r-k$ is also an A-sequence of N for any $k<a_1$.

4. Prove that $r(2n)\leqslant n$ for $n\geqslant 8$ (Erdös and Turán).

This is proved by induction on n and it follows from the formulae $r(2\cdot 8)=8$, $r(2\cdot 9)<9$, $r(2\cdot 10)<10$, $r(2\cdot 11)<11$ and from the implication: if $r(2n)\leqslant n$, then $r(2(n+4))=r(2n+8)\leqslant r(2n)+r(8)\leqslant n+4$.

5. Prove that if $n\geqslant m$, then $r(2n+m-1)\geqslant r(m)+r(n)$ (A. Schinzel).

This follows from the fact that if $a_1<a_2\ldots<a_{r(n)}$ is an A-sequence that belongs to n and $b_1<b_2<\ldots<b_{r(m)}$ is an A-sequence that belongs to m, then, for $n\geqslant m$, $a_1<a_2<\ldots<a_{r(n)}<2a_{r(n)}+b_1-1<2a_{r(n)}+b_2-1<\ldots<2a_{r(n)}+b_{r(m)}-1$ is an A-sequence of the number $2n+m-1$ that consists of $r(n)+r(m)$ terms.

6. Prove that $r(\frac{1}{2}(3^k+1))\geqslant 2^k$ (Erdös and Turán).

The proof is by induction and it follows from the formula $r(\frac{1}{2}(3^0+1))=r(1)=1=2^0$ and from the fact that if $r(\frac{1}{2}(3^k+1))\geqslant 2^k$, then, by exercise 5,

$$r\left(\tfrac{1}{2}(3^{k+1}+1)\right)=r\left(2\left(\tfrac{1}{2}(3^k+1)\right)+\tfrac{1}{2}(3^k+1)-1\right)\geqslant r\left(\tfrac{1}{2}(3^k+1)\right)+r\left(\tfrac{1}{2}(3^k+1)\right)\geqslant 2^{k+1}.$$

7. Prove that $r(51)\geqslant 17$.

The proof follows immediately from the fact (noticed by S. Masłowski) that the sequence 1, 2, 5, 6, 12, 14, 15, 17, 21, 35, 38, 39, 42, 44, 47, 48, 51 does not contain any three numbers in an arithmetical progression.

M. Hall has solved the following problem: does there exist a set Z of different natural numbers such that any natural number is the difference of precisely one pair of numbers of the set Z. We are going to construct an infinite sequence of natural numbers that form a set Z which has the required property (cf. Browkin [2]).

Let $a_1 = 1$, $a_2 = 2$. Further, let n denote a natural number and suppose that the numbers $a_1, a_2, \ldots, a_{2n}$ with $a_1 < a_2 < \ldots a_{2n}$ are already defined. We set $a_{2n+1} = 2a_{2n}$.

Now let r_n be the least natural number which cannot be represented in the form $a_j - a_i$ with $1 \leqslant i < j \leqslant 2n+1$. We define a_{2n+2} as $a_{2n+1} + r_n$. We see that the sequence $a_1, a_2, \ldots$ is now well defined by induction. The initial seven terms of the sequence are 1, 2, 4, 8, 16, 21, 42.

It follows from definition of r_n that each of the numbers $1, 2, \ldots, r_n$ is of the form $a_j - a_i$ with $1 \leqslant i < j \leqslant 2n+2$. Hence it follows that $r_{n+1} > r_n$ for any $n = 1, 2, \ldots$ Therefore any natural number can be represented in the form $a_j - a_i$ provided the indices i, j are suitably chosen.

In order to complete the proof that the set Z indeed has the required property, it remains to show that for any natural numbers h, k, l, m with $h < k$ and $l < m$, $k < m$ the inequality $a_k - a_h \neq a_m - a_l$ is valid. Suppose to the contrary that $a_k - a_h = a_m - a_l$. Since $m > k > h \geqslant 1$, we must have $m \geqslant 3$. If m is odd, i.e. $m = 2n+1$, where n is a natural number, then $a_{2n+1} = a_l + a_k \leqslant 2a_{m-1} = 2a_{2n} = a_{2n+1}$, which is impossible. If m is even, i.e. $m = 2n+2$, where n is a natural number, then, in the case of $l = 2n+1$, we have $a_m - a_l = a_{2n+2} - a_{2n} = r_n$, which, in virtue of the equality $a_k - a_h = a_m - a_l$, gives $r_n = a_k - a_h$, where $h < k \leqslant m-1 = 2n+1$, contrary to the definition of the number r_n. In the case of $l < 2n+1$ (which in virtue of $l < m$ is the only possibility provided $l = 2n+1$ is excluded for $k = 2n+1$), we have $a_m - a_k = a_l - a_h$, whence, since $k < m$, we have $h < l \leqslant 2n$ and $a_m - a_k = a_{2n+2} - a_{2n+1} = r_n$; so $r_n = a_l - a_h$ with $h < l \leqslant 2n$, contrary to the definition of r_n. Finally, if $l < 2n+1$ and $k < 2n+1$, then $a_{2n+2} = a_m = a_l + a_k - a_l < a_l + a_k < a_{2n} + a_{2n} = a_{2n+1}$, which is impossible.

Thus we see that the sequence $a_1, a_2, \ldots$ has the required property.

It will be observed that if the axiom of choice is assumed, a similar property can be proved for real numbers. One can prove the existence of a set X consisting of real numbers and such that any positive real number is uniquely expressible as the difference of two numbers of the set X (1).

§ 5. Odd numbers which are not of the form $2^k + p$, where p is a prime. In the year 1849 A. de Polignac [1] formulated the conjecture that any odd number $n > 1$ is of the form $2^k + p$, where k is a natural number and p is either a prime or the number 1. In 1950 P. Erdös [11] proved that there exist infinitely many odd numbers for which the conjecture fails (cf. also van de Corput [3]).

(1) Cf. Piccard [1], pp. 36-37 (Remarque), and Lindenbaum [1], p. 25, Corollaire 17, and footnote (27) on page 24.

THEOREM 3 (Erdös [11]). *There exists an infinite arithmetical progression of odd numbers none of which is of the form $2^k + p$, where $k = 0, 1, 2, \ldots$, and p is a prime.*

LEMMA. *Every natural number satisfies at least one of the following six congruences:*

(1) $k \equiv 0 \pmod 2$, (2) $k \equiv 0 \pmod 3$, (3) $k \equiv 1 \pmod 4$,

(4) $k \equiv 3 \pmod 8$, (5) $k \equiv 7 \pmod{12}$, (6) $k \equiv 23 \pmod{24}$.

Proof of the lemma. If a number k does not satisfy (1) or (2), then it is divisible neither by 2 nor by 3 and thus it must be of the form $24t + r$, where t is an integer and r is one of the numbers 1, 5, 7, 11, 13, 17, 19, 23. But a straightforward verification shows that then k must satisfy congruences (3), (3), (5), (4), (3), (3), (4), (6), respectively.

COROLLARY. *If k is a non-negative integer, then at least one of the following congruences holds:*

(7) $2^k \equiv 1 \pmod 3$, (8) $2^k \equiv 1 \pmod 7$, (9) $2^k \equiv 2 \pmod 5$,

(10) $2^k \equiv 2^3 \pmod{17}$, (11) $2^k \equiv 2^7 \pmod{13}$, (12) $2^k \equiv 2^{23} \pmod{241}$.

Proof of the corollary. We simply verify that $2^2 \equiv 1 \pmod 3$, $2^3 \equiv 1 \pmod 7$, $2^4 \equiv 1 \pmod 5$, $2^8 \equiv 1 \pmod{17}$, $2^{12} \equiv 1 \pmod{13}$, $2^{12} \equiv -1 \pmod{241}$, whence $2^{24} \equiv 1 \pmod{241}$. From this we infer that the congruences (1), (2), (3), (4), (5), (6) imply the congruences (7,) (8), (9), (10), (11), (12), respectively.

Proof of the theorem. In virtue of the Chinese remainder theorem there exists a natural number a that satisfies the congruences $a \equiv 1 \pmod 2$, $a \equiv 1 \pmod 3$, $a \equiv 1 \pmod 7$, $a \equiv 2 \pmod 5$, $a \equiv 2^3 \pmod{17}$, $a \equiv 2^7 \pmod{13}$, $a \equiv 2^{23} \pmod{241}$, $a \equiv 3 \pmod{31}$ and, moreover, there exists an infinite arithmetical progression of a's each of which satisfies these congruences. Clearly, the terms of the arithmetical progression must be odd. If a is any term of the arithmetical progression, then, since it satisfies the congruences, the corollary of the lemma implies that the number $a - 2^k$ is divisible by at least one of the primes 3, 7, 5, 17, 13, 241. On the other hand, $a \equiv 3 \pmod{31}$ and for any $k = 1, 2, \ldots$ the number 2^k is congruent to one of the numbers 1, 2, 4, 8 (mod 31) (this is because $2^5 \equiv 1 \pmod{31}$). Consequently, $a - 2^k$ is congruent to one of the numbers 2, 1, -9, -5, $-13 \pmod{31}$. But none of these numbers is congruent (mod 31) to any of the numbers 3, 7, 5, 17, 13, 241. Therefore the number $a - 2^k$ cannot possibly be any of these numbers, but, on the other hand, it is divisible by at least one of them. Therefore it is a composite number. Hence it follows that the number $a - 2^k$ cannot be a prime for any non-negative integer k; con-

sequently, a cannot be of the form $a = 2^k+p$, where $k = 0, 1, 2, \ldots$, and p is a prime. Thus we see that the terms of the arithmetical progression which we have defined above have the required property. This proves the truth of theorem 3.

The proof of theorem 3 shows that there exist infinitely many natural numbers n such that for any non-negative integer k the number $-n-2^k$ and thus also the number $n+2^k$ are divisible by at least one of the numbers 3, 7, 5, 17, 13, 241. Let P denote the product of these primes. In virtue of what we proved above the number $n+2^{k[\varphi(P)-1]}$ has a prime divisor $p \mid P$. But $2^{k\varphi(P)} \equiv 1 (\mathrm{mod} P)$, which in virtue of $n+2^{k[\varphi(P)-1]} \equiv 0 (\mathrm{mod} p)$ gives $n \cdot 2^k+1 \equiv 0 (\mathrm{mod} p)$, which for n large enough (e.g. for $n > 241$) gives a composite number $n \cdot 2^k+1$. Thus we have proved the following

COROLLARY. *There exist infinitely many natural numbers n such that each of the numbers $n \cdot 2^k+1$, where $k = 0, 1, 2, \ldots$, is composite* (cf. Sierpiński [27] and Chapter X, § 4, ex. 3).

THEOREM 4 (A. Schinzel). *There exist infinitely many natural numbers that are not representable as sums of two different powers of 2 (with non-negative exponents) and a prime number.*

Proof. (This proof was obtained by A. Schinzel by a thorough examination of the proof of a weaker theorem of R. Crocker [1] which we present below.) We are going to show that the numbers that have the required property are the numbers $2^{2^n}-1$, $n = 3, 4, \ldots$ In fact, suppose that for a natural number $n > 2$ we have $2^{2^n}-1 = 2^k+2^l+p$, where k, l are integers and $k > l \geqslant 0$. We note that the equality $l \equiv 0$ is impossible, because otherwise we would have $p = 2^{2^n}-2^k-2 = 2(2^{2^n-1}-2^{k-1}-1)$ and, since $2^n > k$, $k-1 \leqslant 2^n-2$, whence $2^{2^n-1}-2^{k-1} \geqslant 2^{2^n-1}-2^{2^n-2} = 2^{2^n}-2 \geqslant 2^{2^3-2} = 2^6$, and thus $2^{2^n-1}-2^{k-1}-1 \geqslant 2^6-1 > 1$, which is impossible since p is a prime. Consequently, we have $l \geqslant 1$, and so $k > 1$. Let h denote the greatest non-negative exponent for which 2^h divides $k-l$. The number $(k-l)/2^h$ is then odd and $2^{2^h}+1 \mid 2^{k-l}+1$. Since $p = 2^{2^n}-2^k-2^l-1 = 2^{2^n}-1-2^l(2^{k-l}+1)$, the divisibility relations obtained above give $2^{2^h}+1 \mid p$, whence, in virtue of the fact that p is a prime, we infer that $p = 2^{2^h}+1$. Consequently, $2^{2^n} = 2^k+2^l+2^{2^h}+2$. Since $2^n > k > 1$, the number $2^l+2^{2^h}+2$ is divisible by 4. Therefore either $l = 1$ or $2^h = 1$. If $2^h = 1$, then $l > 1$ and so $2^{2^n-2} = 2^{k-2}+2^{l-2}+1$, which is impossible because the left-hand side of the equality is divisible by 2^6. Thus, necessarily, $l = 1$, $2^h > 1$, whence $2^{2^n-2} = 2^{k-2}+2^{2^h-2}+1$, which (in virtue of $2^n-2 \geqslant 6$) proves that precisely one of the two possible cases $k = 2$ and $2^h = 2$ can occur. If $k = 2$, then $2^h \mid k-l = 1$, which is impossible because $2^h > 1$. If $2^h = 2$, then $k \geqslant 3$ and $2^{2^n-3} = 2^{k-3}+1$, which, in virtue of $n \geqslant 3$, gives $k = 3$, and so $n = 2$, which again is impossible.

This completes the proof of the fact that the numbers $2^{2^n}-1$ have the required property.

COROLLARY (Crocker [1]). *None of the numbers $2^{2^n}-5$, where $n = 3, 4, 5, \ldots$, is of the form 2^k+p, where $k = 0, 1, 2, \ldots$ and p is a prime.*

Proof of the corollary. If $2^{2^n}-5 = 2^k+p$, where k is a non-negative integer and p is a prime, then $2^{2^n}-1 = 2^k+2^2+p$, whence, in view of $n \geqslant 3$, the fact that the numbers $2^{2^n}-1$ have the property just shown implies that k must be equal to 2; consequently $2^{2^n}-1 = 2^3+p$, and so $p = 2^{2^n}-9 = (2^{2^n-1}-3)(2^{2^n+1}+3)$, whence $2^{2^n-1}-3 = 1$, contrary to the assumption that $n \geqslant 3$.