

Chapter 6

Number Theory and Combinatorics

6.1 Arrays of Numbers

Problem 3.4 Prove that the sum of any n entries of the table

$$\begin{array}{ccccc} 1 & \frac{1}{2} & \frac{1}{3} & \cdots & \frac{1}{n} \\ \frac{1}{2} & \frac{1}{3} & \frac{1}{4} & \cdots & \frac{1}{n+1} \\ \vdots & & & & \\ \frac{1}{n} & \frac{1}{n+1} & \frac{1}{n+2} & \cdots & \frac{1}{2n-1} \end{array}$$

situated in different rows and different columns is not less than 1.

Solution Denoting by a_{ij} the entry in the i th row and j th column of the array, we have

$$a_{ij} = \frac{1}{i + j - 1},$$

for all $i, j, 1 \leq i, j \leq n$. Choose n entries situated in different rows and different columns. It follows that from each row and each column exactly one number is chosen. Let $a_{1j_1}, a_{2j_2}, \dots, a_{nj_n}$ be the chosen numbers, where $j_1, j_2, \dots, j_n$ is a permutation of indices $1, 2, \dots, n$. We have

$$\sum_{k=1}^n \frac{1}{a_{kj_k}} = \sum_{k=1}^n (k + j_k - 1) = \sum_{k=1}^n k + \sum_{k=1}^n j_k - n.$$

But

$$\sum_{k=1}^n j_k = \sum_{k=1}^n k = \frac{n(n+1)}{2}$$

since $j_1, j_2, \dots, j_n$ is a permutation of indices $1, 2, \dots, n$. It follows that

$$\sum_{k=1}^n \frac{1}{a_{kj_k}} = n^2.$$

The Cauchy–Schwarz inequality yields

$$(x_1 + x_2 + \dots + x_n) \left(\frac{1}{x_1} + \frac{1}{x_2} + \dots + \frac{1}{x_n} \right) \geq n^2,$$

for all positive real numbers $x_1, x_2, \dots, x_n$. Taking $x_k = a_{kj_k}$ and using the above equality, we obtain

$$\sum_{k=1}^n a_{kj_k} \geq 1$$

as desired.

Problem 3.5 The entries of an $n \times n$ array of numbers are denoted by a_{ij} , $1 \leq i, j \leq n$. The sum of any n entries situated on different rows and different columns is the same. Prove that there exist numbers $x_1, x_2, \dots, x_n$ and $y_1, y_2, \dots, y_n$, such that

$$a_{ij} = x_i + y_j,$$

for all i, j .

Solution Consider n entries situated on different rows and different columns a_{ij_i} , $i = 1, 2, \dots, n$. Fix k and l , $1 \leq k < l \leq n$ and replace a_{kj_k} and a_{lj_l} with a_{kj_l} and a_{lj_k} , respectively. It is not difficult to see that the new n entries are still situated on different rows and different columns. Because the sums of the two sets of n entries are equal, it follows that

$$a_{kj_k} + a_{lj_l} = a_{kj_l} + a_{lj_k}. \quad (*)$$

Now, denote $x_1, x_2, \dots, x_n$ the entries in the first column of the array and by $x_1, x_1 + y_2, x_1 + y_3, \dots, x_1 + y_n$ the entries in the first row (in fact, we have defined $x_k = a_{k1}$, for all k , $y_0 = 0$ and $y_k = a_{1k} - a_{k1}$ for all $k \geq 2$).

x_1	$x_1 + y_2$	$\dots$	$x_1 + y_j$	$\dots$	$x_1 + y_n$
x_2					
$\vdots$					
x_i			a_{ij}		
$\vdots$					
x_n					

The equality

$$a_{ij} = x_i + y_j,$$

stands for all i, j with $i = 1$ or $j = 1$. Now, consider $i, j > 1$. From (*) we deduce

$$a_{11} + a_{ij} = a_{1j} + a_{i1}$$

hence

$$x_1 + a_{ij} = x_i + x_1 + y_j$$

or

$$a_{ij} = x_i + y_j,$$

for all i, j , as desired.

Problem 3.6 In an $n \times n$ array of numbers all rows are different (two rows are different if they differ in at least one entry). Prove that there is a column which can be deleted in such a way that the remaining rows are still different.

Solution We prove by induction on k the following statement: at least $n - k + 1$ columns can be deleted in such a way that the first k rows are still different. For $k = 2$ the assertion is true. Indeed, the first two rows differ in at least one place, so we can delete the remaining $n - 1$ columns. Suppose the assertion is true for k , that is we can delete $n - k + 1$ columns and the first k rows are still different. If after the deletion of the columns the $(k + 1)$ th row is different from all first k rows, we can put back any of the deleted columns and remain with $n - k$ deleted columns and $k + 1$ different rows. If after the deletion the $(k + 1)$ th row coincides with one of the first rows, then we put back the column in which the two rows differ in the original array. For $k = n$ we obtain the desired result.

Problem 3.7 The positive integers from 1 to n^2 ($n \geq 2$) are placed arbitrarily on squares of an $n \times n$ chessboard. Prove that there exist two adjacent squares (having a common vertex or a common side) such that the difference of the numbers placed on them is not less than $n + 1$.

Solution Suppose the contrary: the difference of the numbers placed in any adjacent squares is less than $n + 1$. If we place a king on a square of the chessboard, it can reach any other square in at most $n - 1$ moves through adjacent squares. Place a king in the square with number 1 and move it to the square with number n^2 in at most $n - 1$ moves. At each move, the difference between the numbers in the adjacent squares is less than $n + 1$, hence the difference between n^2 and 1 is less than $(n + 1)(n - 1) = n^2 - 1$, a contradiction.

Problem 3.8 A positive integer is written in each square of an $n^2 \times n^2$ chess board. The difference between the numbers in any two adjacent squares (sharing an edge) is less than or equal to n . Prove that at least $\lfloor \frac{n}{2} \rfloor + 1$ squares contain the same number.

Solution Consider the smallest and largest numbers a and b on the board. They are separated by at most $n^2 - 1$ squares horizontally and $n^2 - 1$ vertically, so there is a path from one to the other with length at most $2(n^2 - 1)$. Then since any two successive squares differ by at most n , we have $b - a \leq 2(n^2 - 1)n$. But since all numbers on the board are integers lying between a and b , only $2(n^2 - 1)n + 1$ distinct numbers can exist; and because

$$n^4 > (2(n^2 - 1)n + 1)\frac{n}{2},$$

more than $\frac{n}{2}$ squares contain the same number, as needed.

Problem 3.9 The numbers $1, 2, \dots, 100$ are arranged in the squares of an 10×10 table in the following way: the numbers $1, \dots, 10$ are in the bottom row in increasing order, numbers $11, \dots, 20$ are in the next row in increasing order, and so on. One can choose any number and two of its neighbors in two opposite directions (horizontal, vertical, or diagonal). Then either the number is increased by 2 and its neighbors are decreased by 1, or the number is decreased by 2 and its neighbors are increased by 1. After several such operations the table again contains all the numbers $1, 2, \dots, 100$. Prove that they are in the original order.

Solution Label the table entry in the i th row and j th column by a_{ij} , where the bottom-left corner is in the first row and first column. Let $b_{ij} = 10(i - 1) + j$ be the number originally in the i th row and j th column.

Observe that

$$P = \sum_{i,j=1}^{10} a_{ij}b_{ij}$$

is invariant. Indeed, every time entries a_{mn}, a_{pq}, a_{rs} are changed (with $m + r = 2p$ and $n + s = 2q$), P increases or decreases by $b_{mn} - 2b_{pq} + b_{rs}$, but this equals

$$10((m - 1) + (r - 1) - 2(p - 1)) + (n + s - 2q) = 0.$$

In the beginning,

$$P = \sum_{i,j=1}^{10} b_{ij}b_{ij}$$

at the end, the entries a_{ij} equal the b_{ij} in some order, and we now have

$$P = \sum_{i,j=1}^{10} a_{ij}b_{ij}$$

By the rearrangement inequality, this is at least $P = \sum_{i,j=1}^{10} a_{ij}b_{ij}$ with equality only when each $a_{ij} = b_{ij}$. The equality does occur since P is invariant. Therefore the a_{ij} do indeed equal the b_{ij} in the same order, and thus the entries $1, 2, \dots, 100$ appear in their original order.

Problem 3.10 Prove that one cannot arrange the numbers from 1 to 81 in a 9×9 table such that for each i , $1 \leq i \leq 9$ the product of the numbers in row i equals the product of the numbers in column i .

Solution The key observation is the following: if row k contains a prime number $p > 40$, then the same number must be contained by column k , as well. Therefore, all prime numbers from 1 to 81 must lie on the main diagonal of the table. However, this is impossible, since there are 10 such prime numbers: 41, 43, 47, 53, 59, 61, 67, 71, 73, and 79.

Problem 3.11 The entries of a matrix are integers. Adding an integer to all entries on a row or on a column is called an operation. It is given that for infinitely many integers N one can obtain, after a finite number of operations, a table with all entries divisible by N . Prove that one can obtain, after a finite number of operations, the zero matrix.

Solution Suppose the matrix has m rows and n columns and its entries are denoted by a_{hk} . Fix some j , $1 < j \leq n$, and consider an arbitrary i , $1 < i \leq m$. The expression

$$E_{ij} = a_{11} + a_{ij} - a_{i1} - a_{1j}$$

is an invariant for our operation. Indeed, adding k to the first row, it becomes

$$(a_{11} + k) + a_{ij} - a_{i1} - (a_{1j} + k) = a_{11} + a_{ij} - a_{i1} - a_{1j}.$$

The same happens if we operate on the first column, the i th row or the j th column, while operating on any other row or column clearly does not change E_{ij} . From the hypothesis, we deduce that E_{ij} is divisible by infinitely positive integers N , hence $E_{ij} = 0$. We deduce that

$$a_{11} - a_{1j} = a_{i1} - a_{ij} = c,$$

for all i , $1 < i \leq m$. Adding c to all entries in column j will make this column identical to the first one.

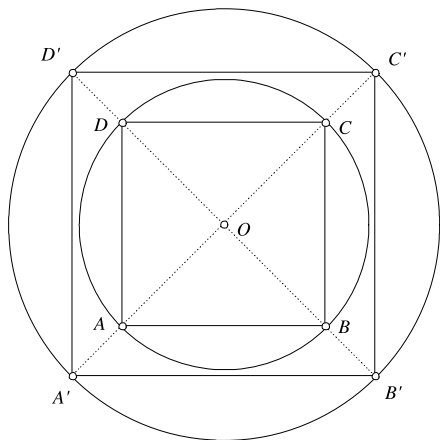
In the same way we can make all columns identical to the first one. Now, it is not difficult to see that operating on rows we can obtain the zero matrix.

6.2 Functions Defined on Sets of Points

Problem 3.14 Let D be the union of $n \geq 1$ concentric circles in the plane. Suppose that the function $f : D \rightarrow D$ satisfies

$$d(f(A), f(B)) \geq d(A, B)$$

for every $A, B \in D$ ($d(M, N)$ is the distance between the points M and N).

Fig. 6.1

Prove that

$$d(f(A), f(B)) = d(A, B)$$

for every $A, B \in D$.

Solution Let $D_1, D_2, \dots, D_n$ be the concentric circles, with radii $r_1 < r_2 < \dots < r_n$ and center O . We will denote $f(A) = A'$, for an arbitrary point $A \in D$.

We first notice that if $A, B \in D_n$ such that AB is a diameter, then $A'B'$ is also a diameter of D_n . If C is another point on D_n , we have

$$A'C'^2 + B'C'^2 \geq AC^2 + BC^2 = AB^2 = A'B'^2.$$

Because OC' is a median of the triangle $A'B'C'$, it follows that

$$OC'^2 = \frac{1}{2}(A'C'^2 + B'C'^2) - \frac{1}{4}A'B'^2 = r_n^2,$$

hence $C' \in D_n$ and $A'C' = AC$, $B'C' = BC$. We deduce that $f(D_n) \subset D_n$ and the restriction of f to D_n is an isometry. Now take A, X, Y, Z on D_n such that $AX = AY = A'Z$. It follows that $A'X' = A'Y' = A'Z$, hence one of the points X', Y' coincides with Z . This shows that $f(D_n) = D_n$ and since f is clearly injective it results in the same way that $f(D_i) = D_i$, for all i , $1 \leq i \leq n-1$, and that all restrictions $f|_{D_i}$ are isometries.

Next we prove that distances between adjacent circles, say D_1 and D_2 are preserved. Take A, B, C, D on D_1 such that $ABCD$ is a square and let A', B', C', D' be the points on D_2 closest to A, B, C, D , respectively.

Then $A'B'C'D'$ is also a square and the distance from A to C' is the maximum between any point on D_1 and any point on D_2 . Hence the eight points maintain their relative position under f and this shows that f is an isometry (Fig. 6.1).

Problem 3.15 Let S be a set of $n \geq 4$ points in the plane, such that no three of them are collinear and not all of them lie on a circle. Find all functions $f : S \rightarrow \mathbf{R}$ with the property that for any circle C containing at least three points of S ,

$$\sum_{P \in C \cap S} f(P) = 0.$$

Solution For two distinct points A, B of S we denote $C_{A,B}$ the set of circles determined by A, B and other points of S . Suppose $C_{A,B}$ has k elements. Since the points of S are not on the same circle, it follows that $k \geq 2$. Because

$$\sum_{P \in C \cap S} f(P) = 0$$

for all $C \in C_{A,B}$, we deduce that

$$\sum_{C \in C_{A,B}} \sum_{P \in C \cap S} f(P) = 0.$$

On the other hand, it is not difficult to see that

$$\sum_{C \in C_{A,B}} \sum_{P \in C \cap S} f(P) = \sum_{P \in S} f(P) + (k-1)(f(A) + f(B)).$$

Thus the sum $\sum_{P \in S} f(P)$ and $f(A) + f(B)$ have opposite signs, for all A, B in S . If, for instance, $\sum_{P \in S} f(P) \geq 0$, then $f(A) + f(B) \leq 0$, for all A, B in S . Let $S = \{A_1, A_2, \dots, A_n\}$. Then

$$f(A_1) + f(A_2) \leq 0, \quad f(A_2) + f(A_3) \leq 0, \dots, \quad f(A_n) + f(A_1) \leq 0,$$

yielding

$$2 \sum_{P \in M} f(P) \leq 0$$

hence $\sum_{P \in M} f(P) = 0$ and $f(A) + f(B) = 0$ for all distinct points A, B . This implies that f is the zero function. Indeed, let A, B, C be three distinct points in S . It is not difficult to see that the equalities

$$f(A) + f(B) = 0,$$

$$f(B) + f(C) = 0,$$

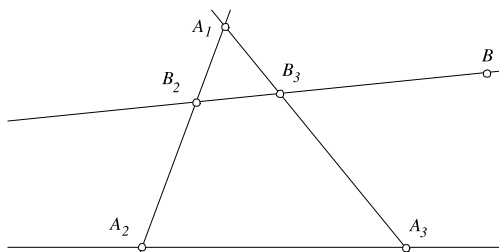
$$f(A) + f(C) = 0$$

yield

$$f(A) = f(B) = f(C) = 0$$

and our claim is proved.

Fig. 6.2



Problem 3.16 Let P be the set of all points in the plane and L be the set of all lines of the plane. Find, with proof, whether there exists a bijective function $f : P \rightarrow L$ such that for any three collinear points A, B, C , the lines $f(A)$, $f(B)$ and $f(C)$ are either parallel or concurrent.

Solution Let $A_i, i = 1, 2, 3$ be three distinct points in the plane and $l_i = f(A_i)$. We claim that if l_1, l_2, l_3 are concurrent or parallel, then A_1, A_2, A_3 are collinear. Indeed, suppose that l_1, l_2, l_3 intersect at M and that $A_1 A_2 A_3$ is a non-degenerated triangle. Then for any point B in the plane we can find points B_2, B_3 on the lines $A_1 A_2, A_1 A_3$, respectively, such that B, B_2, B_3 are collinear (Fig. 6.2).

Because A_1, B_2, A_2 are collinear it follows that $f(B_2)$ is a line passing through M . The same is true for $f(B_1)$, hence also for $f(B)$. This contradicts the surjectivity of f . A similar argument can be given if l_1, l_2, l_3 are parallel.

We conclude that the restriction of f to any line l defines a bijection from l to a pencil of lines (passing through a point or parallel). Consider two pencils P_1 and P_2 of parallel lines. The inverse images of P_1, P_2 are two parallel lines l_1, l_2 (P_1 and P_2 have no common lines, hence l_1 and l_2 have no common points). Let P_3 be a pencil of concurrent lines whose inverse image is a line l , clearly not parallel to l_1, l_2 . Let l' be a line parallel to l . Then $f(l')$ is a pencil of concurrent lines and it follows that there is a line through the points corresponding to l and l' whose inverse image would be a point on both l and l' , a contradiction. Hence no such functions exists.

Problem 3.17 Let S be the set of interior points of a sphere and C be the set of interior points of a circle. Find, with proof, whether there exists a function $f : S \rightarrow C$ such that $d(A, B) \leq d(f(A), f(B))$, for any points $A, B \in S$.

Solution No such function exists. Indeed, suppose $f : S \rightarrow C$ has the enounced property. Consider a cube inscribed in the sphere and assume with no loss of generality that its sides have length 1. Partition the cube into n^3 smaller cubes and let $A_1, A_2, \dots, A_{(n+1)^3}$ be their vertices. For all $i \neq j$ we have

$$d(A_i, A_j) \geq \frac{1}{n},$$

hence

$$d(f(A_i), f(A_j)) \geq \frac{1}{n}.$$

It follows that the disks D_i with centers $f(A_i)$ and radius $\frac{1}{2n}$ are disjoint and contained in a circle C' with radius $r + \frac{1}{n}$, where r is the radius of C . The sum of the areas of these disks is then less than the area of C' , hence

$$(n+1)^3 \frac{\pi}{4n^2} \leq \pi \left(r + \frac{1}{n} \right)^2.$$

This inequality cannot hold for sufficiently large n , which proves our claim.

Problem 3.18 Let S be the set of all polygons in the plane. Prove that there exists a function $f : S \rightarrow (0, +\infty)$ such that

1. $f(P) < 1$, for any $P \in S$;
2. If $P_1, P_2 \in S$ have disjoint interiors and $P_1 \cup P_2 \in S$, then $f(P_1 \cup P_2) = f(P_1) + f(P_2)$.

Solution Consider a covering of the plane with unit squares and denote them by $U_1, U_2, \dots, U_n, \dots$. If P is a polygon, define

$$f(P) = \sum_{k \geq 1} \frac{1}{2^k} [P \cap U_k].$$

Because P intersects a finite number of unit squares, the above sum is finite, hence f is well defined. Moreover, f verifies the conditions of the problem. Indeed, we have $[P \cap U_k] \leq 1$, for all k and if

$$N = \max\{i \mid P \cap U_i \neq \emptyset\}$$

then

$$f(P) = \sum_{k \geq 1} \frac{1}{2^k} [P \cap U_k] \leq \sum_{k \geq 1} \frac{1}{2^k} = 1 - \frac{1}{2^N} < 1.$$

For the second condition, observe that

$$[(P_1 \cap P_2) \cap U_k] = [P_1 \cap U_k] + [P_2 \cap U_k]$$

for all polygons P_1, P_2 for which $P_1 \cup P_2 \in S$ and all U_k , hence

$$f(P_1 \cup P_2) = f(P_1) + f(P_2).$$

6.3 Count Twice!

Problem 3.22 Find how many committees with a chairman can be chosen from a set of n persons. Derive the identity

$$\binom{n}{1} + 2\binom{n}{2} + 3\binom{n}{3} + \dots + n\binom{n}{n} = n2^{n-1}.$$

Solution The number of persons in the committee may vary between 1 and n . Let us count how many such committees number k persons. The k persons can be chosen in $\binom{n}{k}$ ways while the chairman can be chosen in k ways, yielding a total of $k\binom{n}{k}$ committees with k persons. Adding up for $k = 1, 2, \dots, n$, we see that the total number of committees is

$$\binom{n}{1} + 2\binom{n}{2} + 3\binom{n}{3} + \cdots + n\binom{n}{n}.$$

On the other hand, we can first choose the chairman. This can be done in n ways. Next, we choose the rest of the committee, which is an arbitrary subset of the remaining $n - 1$ persons. Because a set with $n - 1$ elements contains 2^{n-1} subsets, it follows that the committee can be completed in 2^{n-1} ways and the total number of committees is

$$n2^{n-1}.$$

Observation There are many proofs of the given equality. An interesting one is the following. Consider the identity

$$(1+x)^n = 1 + \binom{n}{1}x + \binom{n}{2}x^2 + \cdots + \binom{n}{n-1}x^{n-1} + \binom{n}{n}x^n.$$

Differentiating both sides with respect to x yields

$$n(1+x)^{n-1} = \binom{n}{1} + 2\binom{n}{2}x + \cdots + (n-1)\binom{n}{n-1}x^{n-2} + n\binom{n}{n}x^{n-1}.$$

Setting $x = 1$ gives the desired result.

Problem 3.23 In how many ways can one choose k balls from a set containing $n - 1$ red balls and a blue one? Derive the identity

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

Solution We have to choose k balls from a set containing n balls, hence the answer is $\binom{n}{k}$. On the other hand, the blue ball may or may not be among the selected k balls. If the blue ball is selected, then, in fact we have chosen $k - 1$ red balls from $n - 1$ red balls and this can be done in $\binom{n-1}{k-1}$ ways. If the blue ball is not selected, then we have chosen k red balls from $n - 1$ ones. This can be done in $\binom{n-1}{k}$ which leads to a total of

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

possibilities to choose the k balls.

Observation Using similar arguments we can obtain a more general identity. Let us count in how many ways one can choose k balls from a set containing n red and m blue balls. Discarding the color of the balls, the answer is $\binom{n+m}{k}$. If we take into consideration the fact that the chosen k balls can be: all red, or $k-1$ red and 1 blue, or $k-2$ red and 2 blue, etc. we obtain the identity

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

Problem 3.24 Let S be a set of n persons such that:

- (i) any person is acquainted to exactly k other persons in S ;
- (ii) any two persons that are acquainted have exactly l common acquaintances in S ;
- (iii) any two persons that are not acquainted have exactly m common acquaintances in S .

Prove that

$$m(n-k) - k(k-l) + k - m = 0.$$

Solution Let a be a fixed element of S . Let us count the triples (a, x, y) such that a, x are acquainted, x, y are acquainted and a, y are not acquainted. Because a is acquainted to exactly k other persons in S , x can be chosen in k ways and for fixed a and x , y can be chosen in $k-1-l$ ways. Thus the number of such triples is

$$k(k-1-l).$$

Let us count again, choosing y first. The number of persons not acquainted to a equals $n-k-1$, hence y can be chosen in $n-k-1$ ways. Because x is a common acquaintance of a and y , it can be chosen in m ways, yielding a total of

$$m(n-k-1)$$

triples. It is not difficult to see that the equality

$$k(k-1-l) = m(n-k-1)$$

is equivalent to the desired one.

Problem 3.25 Let n be an odd integer greater than 1 and let $c_1, c_2, \dots, c_n$ be integers. For each permutation $a = (a_1, a_2, \dots, a_n)$ of $\{1, 2, \dots, n\}$, define

$$S(a) = \sum_{i=1}^n c_i a_i.$$

Prove that there exist permutations $a \neq b$ of $\{1, 2, \dots, n\}$ such that $n!$ is a divisor of $S(a) - S(b)$.

Solution Denote by $\sum_a S(a)$ the sum of $S(a)$ over all $n!$ permutations of $\{1, 2, \dots, n\}$. We compute $\sum_a S(a) \pmod{n!}$ in two ways. First, assuming that the conclusion is false, it follows that each $S(a)$ has a different remainder mod $n!$, hence these remainders are the numbers $0, 1, 2, \dots, n! - 1$. It follows that

$$\sum_a S(a) \equiv \frac{1}{2}n!(n! - 1) \pmod{n!}.$$

On the other hand,

$$\sum_a S(a) = \sum_a \sum_{i=1}^n c_i a_i = \sum_{i=1}^n c_i \sum_a a_i.$$

For each i , in $\sum_a a_i$, each of the numbers $1, 2, \dots, n$, appears $(n-1)!$ times, hence

$$\sum_a a_i = (n-1)!(1 + 2 + \dots + n) = \frac{1}{2}(n+1)!.$$

It follows that

$$\sum_a S(a) = \frac{1}{2}(n+1)! \sum_{i=1}^n c_i.$$

We deduce that

$$\frac{1}{2}n!(n! - 1) \equiv \frac{1}{2}(n+1)! \sum_{i=1}^n c_i \pmod{n!}.$$

Because $n > 1$ is odd, the right-hand side is congruent to $0 \pmod{n!}$, while the left-hand side is not, a contradiction.

Problem 3.26 Let $a_1 \leq a_2 \leq \dots \leq a_n = m$ be positive integers. Denote by b_k the number of those a_i for which $a_i \geq k$. Prove that

$$a_1 + a_2 + \dots + a_n = b_1 + b_2 + \dots + b_m.$$

Solution Let us consider a $n \times m$ array of numbers (x_{ij}) defined as follows: in row i , the first a_i entries are equal to 1 and the remaining $m - a_i$ entries are equal to 0. For instance, if $n = 3$ and $a_1 = 2, a_2 = 4, a_3 = 5$, the array is

1	1	0	0	0
1	1	1	1	0
1	1	1	1	1

Now, if we examine column j , we notice that the number of 1's in that column equals the number of those a_i greater than or equal to j , hence b_j . The desired result follows by adding up in two ways the 1's in the array. The total number of 1's is $\sum_{i=1}^n a_i$, if counted by rows, and $\sum_{j=1}^m b_j$, if counted by columns.

Problem 3.27 In how many ways can one fill a $m \times n$ table with ± 1 such that the product of the entries in each row and each column equals -1 ?

Solution Denote by a_{ij} the entries in the table. For $1 \leq i \leq m-1$ and $1 \leq j \leq n-1$, we let $a_{ij} = \pm 1$ in an arbitrary way. This can be done in $2^{(m-1)(n-1)}$ ways. The values for a_{mj} with $1 \leq j \leq n-1$ and for a_{in} , with $1 \leq i \leq m-1$ are uniquely determined by the condition that the product of the entries in each row and each column equals -1 . The value of a_{mn} is also uniquely determined but it is necessary that

$$\prod_{j=1}^{n-1} a_{mj} = \prod_{i=1}^{m-1} a_{in}. \quad (*)$$

If we denote

$$P = \prod_{i=1}^{m-1} \prod_{j=1}^{n-1} a_{ij}$$

we observe that

$$P \prod_{j=1}^{n-1} a_{mj} = (-1)^{n-1}$$

and

$$P \prod_{i=1}^{m-1} a_{in} = (-1)^{m-1}$$

hence $(*)$ holds if and only if m and n have the same parity.

Problem 3.28 Let n be a positive integer. Prove that

$$\sum_{k=0}^n \binom{n}{k} \binom{n+k}{k} = \sum_{k=0}^n 2^k \binom{n}{k}^2.$$

Solution Let us count in two ways the number of ordered pairs (A, B) , where A is a subset of $\{1, 2, \dots, n\}$, and B is a subset of $\{1, 2, \dots, 2n\}$ with n elements and disjoint from A .

First, for $0 \leq k \leq n$, choose a subset A of $\{1, 2, \dots, n\}$ having $n - k$ elements. This can be done in

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

ways. Next, choose B , a subset with n elements of $\{1, 2, \dots, 2n\} - A$. Since $\{1, 2, \dots, 2n\} - A$ has $2n - (n - k) = n + k$ elements, B can be chosen in

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

ways. We deduce, by adding on k , that the number of such pairs equals

$$\sum_{k=0}^n \binom{n}{k} \binom{n+k}{k}.$$

On the other hand, we could start by choosing the subsets $B' \subset \{1, 2, \dots, n\}$ and $B'' \subset \{n+1, n+2, \dots, 2n\}$, both with k elements, and define

$$B = B'' \cup (\{1, 2, \dots, n\} - B').$$

Since for given k each of the sets B' and B'' can be chosen in $\binom{n}{k}$ ways, B can be chosen in $\binom{n}{k}^2$ ways.

Finally, pick A to be an arbitrary subset of B' . There are 2^k ways to do this. Adding on k , we obtain that the total number of pairs (A, B) equals

$$\sum_{k=0}^n 2^k \binom{n}{k}^2,$$

hence the conclusion.

Problem 3.29 Prove that

$$1^2 + 2^2 + \dots + n^2 = \binom{n+1}{2} + 2 \binom{n+1}{3}.$$

Solution Let us count the number of ordered triples of integers (a, b, c) satisfying $0 \leq a, b < c \leq n$.

For fixed c , a and b can independently take values in the set $\{0, 1, \dots, c-1\}$, hence there are c^2 such triples. Since c can take any integer value between 1 and n , the total number of triples equals

$$1^2 + 2^2 + \dots + n^2.$$

On the other hand, there are $\binom{n+1}{2}$ triples of the form (a, a, c) and $2\binom{n+1}{3}$ triples (a, b, c) with $a \neq b$. The latter results from the following argument: we can choose three distinct elements from $\{0, 1, \dots, n\}$ in $\binom{n+1}{3}$ ways. With these three elements, say $x < y < z$, we can form two triples satisfying the required condition: (x, y, z) and (y, x, z) .

Problem 3.30 Let n and k be positive integers and let S be a set of n points in the plane such that

- (a) no three points of S are collinear, and
- (b) for every point P of S there are at least k points of S equidistant from P .

Prove that

$$k < \frac{1}{2} + \sqrt{2n}.$$

Solution Let $P_1, P_2, \dots, P_n$ be the given points. Let us estimate the number of isosceles triangles whose vertices lie in S .

For each P_i , there are at least $\binom{k}{2}$ triangles $P_i P_j P_k$, with $P_i P_j = P_i P_k$, hence the total number of isosceles triangles is at least $n\binom{k}{2}$.

For each pair (P_i, P_j) , with $i \neq j$, there exist at most two points in S equidistant from P_i and P_j . This is because all such points lie on the perpendicular bisector of the line segment $P_i P_j$ and no three points of S are collinear. Thus, the total number of isosceles triangles is at most $2\binom{n}{2}$. We deduce that

$$n\binom{k}{2} \leq 2\binom{n}{2},$$

which simplifies to

$$2(n-1) \geq k(k-1).$$

Suppose, by way of contradiction, that

$$k \geq \frac{1}{2} + \sqrt{2n}.$$

Then

$$k(k-1) \geq \left(\sqrt{2n} + \frac{1}{2}\right)\left(\sqrt{2n} - \frac{1}{2}\right) = 2n - \frac{1}{4} > 2(n-1),$$

a contradiction.

Problem 3.31 Prove that

$$\tau(1) + \tau(2) + \dots + \tau(n) = \left\lfloor \frac{n}{1} \right\rfloor + \left\lfloor \frac{n}{2} \right\rfloor + \dots + \left\lfloor \frac{n}{n} \right\rfloor,$$

where $\tau(k)$ denotes the number of divisors of the positive integer k .

Solution Observe that the integer a , with $1 \leq a \leq n$, is counted by $\tau(k)$ if and only if a is a divisor of k , or, equivalently, if k is a multiple of a . Thus, the number of times a is counted in the left-hand side of our equality equals the number of multiples of a in the set $\{1, 2, \dots, n\}$. But this number obviously equals $\left\lfloor \frac{n}{a} \right\rfloor$. Adding on a gives the desired result.

Problem 3.32 Prove that

$$\sigma(1) + \sigma(2) + \dots + \sigma(n) = \left\lfloor \frac{n}{1} \right\rfloor + 2\left\lfloor \frac{n}{2} \right\rfloor + \dots + n\left\lfloor \frac{n}{n} \right\rfloor,$$

where $\sigma(k)$ denotes the sum of divisors of the positive integer k .

Solution The solution is similar to the previous one. The integer a , with $1 \leq a \leq n$, is a term of the sum $\sigma(k)$ if and only if a is a divisor of k . There are $\lfloor \frac{n}{a} \rfloor$ multiples of a in the set $\{1, 2, \dots, n\}$ and therefore the sum of all divisors equal to a is $a \lfloor \frac{n}{a} \rfloor$.

Problem 3.33 Prove that

$$\varphi(1) \left\lfloor \frac{n}{1} \right\rfloor + \varphi(2) \left\lfloor \frac{n}{2} \right\rfloor + \cdots + \varphi(n) \left\lfloor \frac{n}{n} \right\rfloor = \frac{n(n+1)}{2},$$

where φ denotes Euler's totient function.

Solution Observe that the right-hand side can be written as

$$\frac{n(n+1)}{2} = 1 + 2 + \cdots + n.$$

Using the result of Problem 3.21 of Sect. 3.3, we obtain

$$\frac{n(n+1)}{2} = \sum_{d|1} \varphi(d) + \sum_{d|2} \varphi(d) + \cdots + \sum_{d|n} \varphi(d).$$

Now, for some k , $1 \leq k \leq n$, let us count how many times $\varphi(k)$ appears in right-hand side of the above equality. Clearly, $\varphi(k)$ is a term of the sum $\sum_{d|m} \varphi(d)$ if and only if k is a divisor of m , or, equivalently, m is a multiple of k . So, $\varphi(k)$ appears as many times as the number of multiples of k in the set $\{1, 2, \dots, n\}$, that is, $\lfloor \frac{n}{k} \rfloor$.

We conclude that the sum can be written as

$$\varphi(1) \left\lfloor \frac{n}{1} \right\rfloor + \varphi(2) \left\lfloor \frac{n}{2} \right\rfloor + \cdots + \varphi(n) \left\lfloor \frac{n}{n} \right\rfloor,$$

giving the required result.

Alternatively, we could count in two ways the number of fractions $\frac{a}{b}$ with $1 \leq a \leq b \leq n$ where we do not insist that our fraction be in lowest terms, so for example $\frac{1}{2}$ and $\frac{2}{4}$ would count as different fractions. First, this number is clearly

$$\sum_{b=1}^n b = \frac{n(n+1)}{2}$$

since this is the number of such pairs (a, b) . Second, we count fractions based on their reduced forms. We saw in Problem 3.21 that the number of reduced fractions with denominator d is $\phi(d)$. The number of multiples of such a fraction with denominator at most n is $\lfloor n/d \rfloor$ so the number is also

$$\sum_{d=1}^n \phi(d) \left\lfloor \frac{n}{d} \right\rfloor.$$

6.4 Sequences of Integers

Problem 3.37 Prove that there exist sequences of odd integers $(x_n)_{n \geq 3}, (y_n)_{n \geq 3}$ such that

$$7x_n^2 + y_n^2 = 2^n$$

for all $n \geq 3$.

Solution For $n = 3$, define $x_3 = y_3 = 1$. Suppose that for $n \geq 3$ there exist odd integers x_n and y_n such that $7x_n^2 + y_n^2 = 2^n$. Observe that the integers

$$\frac{x_n + y_n}{2} \quad \text{and} \quad \frac{x_n - y_n}{2}$$

cannot be both even, since their sum is odd.

If $\frac{x_n + y_n}{2}$ is odd, we define

$$x_{n+1} = \frac{x_n + y_n}{2}, \quad y_{n+1} = \frac{7x_n - y_n}{2}$$

and the conclusion follows by noticing that

$$7x_{n+1}^2 + y_{n+1}^2 = \frac{1}{4}(7(x_n + y_n)^2 + (7x_n - y_n)^2) = 2(7x_n^2 + y_n^2) = 2^{n+1}.$$

If $\frac{x_n - y_n}{2}$ is odd, we define

$$x_{n+1} = \frac{x_n - y_n}{2}, \quad y_{n+1} = \frac{7x_n + y_n}{2}$$

and a similar computation yields the result.

Problem 3.38 Let $x_1 = x_2 = 1, x_3 = 4$ and

$$x_{n+3} = 2x_{n+2} + 2x_{n+1} - x_n$$

for all $n \geq 1$. Prove that x_n is a square for all $n \geq 1$.

Solution We first notice that $x_1 = x_2 = 1^2, x_3 = 2^2, x_4 = 3^2, x_5 = 5^2, x_6 = 8^2$, and so forth. This leads to the assumption that $x_n = F_n^2$, where F_n is the n th term of the Fibonacci sequence defined by $F_1 = F_2 = 1$ and $F_{n+1} = F_n + F_{n-1}$, for all $n \geq 2$. We prove this assertion inductively. Suppose it is true for all $k \leq n + 2$. Then

$$\begin{aligned} x_{n+3} &= 2F_{n+2}^2 + 2F_{n+1}^2 - F_n^2 = 2F_{n+2}^2 + 2F_{n+1}^2 - (F_{n+2} - F_{n+1})^2 \\ &= F_{n+2}^2 + F_{n+1}^2 + 2F_{n+1}F_{n+2} = (F_{n+2} + F_{n+1})^2 = F_{n+3}^2, \end{aligned}$$

and the assertion is proved.

Problem 3.39 The sequence $(a_n)_{n \geq 0}$ is defined by $a_0 = a_1 = 1$ and

$$a_{n+1} = 14a_n - a_{n-1}$$

for all $n \geq 1$. Prove that the number $2a_n - 1$ is a square for all $n \geq 0$.

Solution We have $2a_0 - 1 = 1$, $2a_1 - 1 = 1$, $2a_2 - 1 = 5^2$, $2a_3 - 1 = 19^2$, $2a_4 - 1 = 71^2$. We observe that if we define $b_0 = -1$, $b_1 = 1$, $b_2 = 5$, $b_3 = 19$, $b_4 = 71$, then $b_{n+1} = 4b_n - b_{n-1}$ for $1 \leq n \leq 3$. We will prove inductively that

$$2a_n - 1 = b_n^2,$$

where $b_0 = -1$, $b_1 = 1$ and $b_{n+1} = 4b_n - b_{n-1}$ for all $n \geq 1$. Suppose this is true for $1, 2, \dots, n$ and observe that

$$\begin{aligned} 2a_{n+1} - 1 &= 14(2a_n - 1) - (2a_{n-1} - 1) + 12 = 14b_n^2 - b_{n-1}^2 + 12 \\ &= 16b_n^2 - 8b_nb_{n-1} + b_{n-1}^2 - 2b_n^2 + 8b_nb_{n-1} - 2b_{n-1}^2 + 12 \\ &= (4b_n - b_{n-1})^2 - 2(b_n^2 + b_{n-1}^2 - 4b_nb_{n-1} - 6) \\ &= b_{n+1}^2 - 2(b_n^2 + b_{n-1}^2 - 4b_nb_{n-1} - 6). \end{aligned}$$

Hence it suffices to prove that $b_n^2 + b_{n-1}^2 - 4b_nb_{n-1} - 6 = 0$. This follows also by induction. It is true for $n = 1$ and $n = 2$. Suppose it holds for n and observe that

$$\begin{aligned} b_{n+1}^2 + b_n^2 - 4b_{n+1}b_n - 6 &= (4b_n - b_{n-1})^2 + b_n^2 - 4(4b_n - b_{n-1})b_n - 6 \\ &= b_n^2 + b_{n-1}^2 - 4b_nb_{n-1} - 6 = 0, \end{aligned}$$

as desired.

Problem 3.40 The sequence $(x_n)_{n \geq 1}$ is defined by $x_1 = 0$ and

$$x_{n+1} = 5x_n + \sqrt{24x_n^2 + 1}$$

for all $n \geq 1$. Prove that all x_n are positive integers.

Solution We first notice that the sequence is increasing and all of its terms are positive. Next we observe that the recursive relation is equivalent to

$$x_{n+1}^2 - 10x_nx_{n+1} + x_n^2 - 1 = 0.$$

Replacing n by $n - 1$ yields

$$x_n^2 - 10x_nx_{n-1} + x_{n-1}^2 - 1 = 0,$$

hence for $n \geq 2$ the numbers x_{n+1} and x_{n-1} are distinct roots of the equation

$$x^2 - 10x_nx + x_n^2 - 1 = 0.$$

The Viète's relations yield $x_{n+1} + x_{n-1} = 10x_n$, or

$$x_{n+1} = 10x_n - x_{n-1}$$

for all $n \geq 2$. Because $x_1 = 1$ and $x_2 = 10$, it follows inductively that all x_n are positive integers.

Problem 3.41 Let $(a_n)_{n \geq 1}$ be an increasing sequence of positive integers such that

1. $a_{2n} = a_n + n$ for all $n \geq 1$;
2. if a_n is a prime, then n is a prime.

Prove that $a_n = n$, for all $n \geq 1$.

Solution Let $a_1 = c$. Then $a_2 = a_1 + 1 = c + 1$, $a_4 = a_2 + 2 = c + 3$. Since the sequence is increasing, it follows that $a_3 = c + 2$. We prove that $a_n = c + n - 1$ for all $n \geq 1$. Indeed, if $n = 2^k$ for some integer k this follows by induction on k . Suppose that

$$a_{2^k} = c + 2^k - 1.$$

Then

$$a_{2^{k+1}} = a_{2 \cdot 2^k} = a_{2^k} + 2^k = c + 2^{k+1} - 1.$$

If $2^k < n < 2^{k+1}$, then

$$c + 2^k - 1 = a_{2^k} < a_{2^k+1} < \cdots < a_n < \cdots < a_{2^{k+1}} = c + 2^{k+1} - 1$$

and this is possible only if $a_n = c + n - 1$.

Next we prove that $c = 1$. Suppose that $c \geq 2$ and let $p < q$ be two consecutive prime numbers greater than c . We have

$$a_{q-c+1} = c + q - c = q,$$

hence $q - c + 1$ is a prime and clearly $q - c + 1 \leq p$. It follows that for any consecutive prime numbers $p < q$ we have

$$q - p \leq c - 1.$$

The numbers $(c+1)! + 2, (c+1)! + 3, \dots, (c+1)! + c + 1$ are all composite, hence if p and q are the consecutive primes such that

$$p < (c+1)! + 2 < (c+1)! + c + 1 < q$$

then

$$q - p > c - 1,$$

a contradiction. It follows that $c = 1$ and $a_n = n$ for all $n \geq 1$.

Problem 3.42 Let $a_0 = a_1 = 1$ and $a_{n+1} = 2a_n - a_{n-1} + 2$, for all $n \geq 1$. Prove that

$$a_{n^2+1} = a_{n+1}a_n,$$

for all $n \geq 0$.

Solution We will find a closed form for a_n . Denoting $b_n = a_{n+1} - a_n$, we observe that the given recursive equation becomes

$$b_n = b_{n-1} + 2,$$

thus $(b_n)_{n \geq 0}$ is an arithmetic sequence and hence $b_n = b_0 + 2n = 2n$. Writing $a_{k+1} - a_k = 2(k-1)$ for $k = 1, 2, \dots, n-1$ and adding up yield $a_n = n^2 - n + 1$, for all $n \geq 0$. Now, an elementary computation shows that

$$a_{n^2+1} = (n^2 + 1)^2 - (n^2 + 1) + 1 = (n^2 + n + 1)(n^2 - n + 1) = a_{n+1}a_n,$$

as desired.

Problem 3.43 Let $a_0 = 1$ and $a_{n+1} = a_0 \cdots a_n + 4$, for all $n \geq 0$. Prove that

$$a_n - \sqrt{a_{n+1}} = 2,$$

for all $n \geq 1$.

Solution We will prove the equivalent statement

$$a_{n+1} = (a_n - 2)^2.$$

We have

$$\begin{aligned} a_{n+1} &= a_0 \cdots a_{n-1} \cdot a_n + 4 \\ &= (a_n - 4) \cdot a_n + 4 \\ &= a_n^2 - 4a_n + 4 \\ &= (a_n - 2)^2, \end{aligned}$$

which concludes the proof.

Problem 3.44 The sequence $(x_n)_{n \geq 1}$ is defined by $x_1 = 1, x_2 = 3$ and $x_{n+2} = 6x_{n+1} - x_n$, for all $n \geq 1$. Prove that $x_n + (-1)^n$ is a perfect square, for all $n \geq 1$.

Solution Let $y_n = x_n + (-1)^n$. By inspection, we find that $y_1 = 0, y_2 = 4, y_3 = 16, y_4 = 100, y_5 = 576$ etc. Denote by $z_n = \sqrt{y_n}$; then $z_1 = 0, z_2 = 2, z_3 = 4, z_4 = 10, z_5 = 24$, and so on. The first terms of the sequence $(z_n)_{n \geq 1}$ suggest that $z_{n+2} = 2z_{n+1} + z_n$, for all $n \geq 1$. Indeed, we will prove by induction the following statement: $y_n = z_n^2$, where $z_1 = 0, z_2 = 2$ and $z_{n+2} = 2z_{n+1} + z_n$, for all $n \geq 1$.

The base case is easy to deal with. In order to prove the inductive step, we need a recursive equation for the sequence $(y_n)_{n \geq 1}$. Since $x_n = y_n - (-1)^n$, we have

$$y_{n+2} - (-1)^{n+2} = 6y_{n+1} - 6(-1)^{n+1} - y_n + (-1)^n,$$

and also

$$y_{n+1} - (-1)^{n+1} = 6y_n - 6(-1)^n - y_{n-1} + (-1)^{n-1}.$$

Adding up yields

$$y_{n+2} + y_{n+1} = 6y_{n+1} + 6y_n - y_n - y_{n-1},$$

or

$$y_{n+2} = 5y_{n+1} + 5y_n - y_{n-1},$$

for all $n \geq 2$. Now, we are ready to prove the inductive step. Assume $y_k = z_k^2$, for $k = 1, 2, \dots, n+1$. Then

$$\begin{aligned} y_{n+2} &= 5z_{n+1}^2 + 5z_n^2 - z_{n-1}^2 \\ &= 5z_{n+1}^2 + 5z_n^2 - (z_{n+1} - 2z_n)^2 \\ &= 4z_{n+1}^2 + z_n^2 + 4z_{n+1}z_n \\ &= (2z_{n+1} + z_n)^2 \\ &= z_{n+2}^2, \end{aligned}$$

and we are done.

Observation The informed reader may notice that an alternative solution is possible if we write x_n in closed form. Indeed, it is known that if α and β , with $\alpha \neq \beta$, are the roots of the quadratic equation

$$x^2 = ax + b,$$

then any sequence satisfying

$$x_{n+2} = ax_{n+1} + bx_n,$$

for all $n \geq 1$, has the form

$$x_n = c_1\alpha^n + c_2\beta^n,$$

where the constants c_1 and c_2 can be determined from the first two terms of the sequence. In our case, the roots of the equation

$$x^2 = 6x - 1$$

are

$$\alpha = 3 + 2\sqrt{2}, \quad \beta = 3 - 2\sqrt{2},$$

hence

$$x_n = c_1(3 + 2\sqrt{2})^n + c_2(3 - 2\sqrt{2})^n.$$

Since $x_1 = 1$ and $x_2 = 3$, we obtain

$$c_1 = \frac{1}{2}(3 - 2\sqrt{2}), \quad c_2 = \frac{1}{2}(3 + 2\sqrt{2}),$$

hence

$$x_n = \frac{1}{2}((3 + 2\sqrt{2})^{n-1} + (3 - 2\sqrt{2})^{n-1}),$$

for all $n \geq 1$. It follows that

$$\begin{aligned} x_n + (-1)^n &= \frac{1}{2}((3 + 2\sqrt{2})^{n-1} + (3 - 2\sqrt{2})^{n-1} + 2(-1)^n) \\ &= \frac{1}{2}((1 + \sqrt{2})^{2(n-1)} + (1 - \sqrt{2})^{2(n-1)} - 2(-1)^{n-1}) \\ &= \left(\frac{(1 + \sqrt{2})^{n-1} - (1 - \sqrt{2})^{n-1}}{\sqrt{2}} \right)^2. \end{aligned}$$

The sequence

$$w_n = \frac{(1 + \sqrt{2})^{n-1} - (1 - \sqrt{2})^{n-1}}{\sqrt{2}}$$

has the form

$$w_n = c_1\alpha^n + c_2\beta^n,$$

with

$$\alpha = 1 + \sqrt{2}, \quad \beta = 1 - \sqrt{2},$$

hence it satisfies the recursive equation

$$w_{n+2} = 2w_{n+1} + w_n,$$

for all $n \geq 1$. Finally, since $w_1 = 0$ and $w_2 = 2$, we deduce that w_n is an integer for all $n \geq 1$.

Problem 3.45 Let $(a_n)_{n \geq 1}$ be a sequence of non-negative integers such that $a_n \geq a_{2n} + a_{2n+1}$, for all $n \geq 1$. Prove that for any positive integer N we can find N consecutive terms of the sequence, all equal to zero.

Solution Let us first show that at least one term of the sequence equals zero. Suppose the contrary, that is, all terms are positive integers. But then

$$a_1 \geq a_2 + a_3 \geq a_4 + a_5 + a_6 + a_7 \geq \cdots \geq a_{2^n} + a_{2^n+1} + \cdots + a_{2^{n+1}-1} \geq 2^n,$$

for all $n \geq 1$, which is absurd. Thus, at least one term, say a_k , equals zero. But then

$$0 = a_k \geq a_{2k} + a_{2k+1} \geq \cdots \geq a_{2^n k} + a_{2^n k+1} + \cdots + a_{2^n k+2^n-1},$$

hence $a_{2^n k} = a_{2^n k+1} = \cdots = a_{2^n k+2^n-1} = 0$. We found 2^n consecutive terms of our sequence, all equal to zero, which clearly proves the claim.

Observation An nontrivial example of such a sequence is the following:

$$a_n = \begin{cases} 1, & \text{if } n = 2^k, \text{ for some integer } k, \\ 0, & \text{otherwise.} \end{cases}$$

6.5 Equations with Infinitely Many Solutions

Problem 3.48 Find all triples of integers (x, y, z) such that

$$x^2 + xy = y^2 + xz.$$

Solution The given equation is equivalent to

$$x(x - z) = y(y - x).$$

Denote by $d = \gcd(x, y)$. Then $x = da$, $y = db$, with $\gcd(a, b) = 1$. We deduce that $y - x = ka$ and $x - z = kb$ for some integer k . Because $\gcd(a, b - a) = \gcd(a, b) = 1$, it follows that $b - a$ divides k . Setting $k = m(b - a)$ we obtain $d = ma$ and the solutions are

$$x = ma^2, \quad y = mab, \quad z = m(a^2 + ab - b^2)$$

where m, a, b are arbitrary integers.

Problem 3.49 Let n be an integer number. Prove that the equation

$$x^2 + y^2 = n + z^2$$

has infinitely many integer solutions.

Solution The equation is equivalent to

$$(x - z)(x + z) + y^2 = n.$$

If we set $x - z = 1$, then we obtain

$$2x - 1 + y^2 = n$$

and

$$x = \frac{n + 1 - y^2}{2}.$$

Now, it suffices to take $y = n + m$, where m is an odd integer to insure that x is an integer as well. Indeed, if $m = 2k + 1$, then

$$\frac{n + 1 - y^2}{2} = \frac{n + 1 - (n + 2k + 1)^2}{2} = -\frac{n(n + 1)}{2} - 2nk - 2k^2 - 2k,$$

obviously an integer. Since $z = x - 1$, it is also an integer number.

Problem 3.50 Let m be a positive integer. Find all pairs of integers (x, y) such that

$$x^2(x^2 + y) = y^{m+1}.$$

Solution Multiplying the equation by 4 and adding y^2 to both sides yields the equivalent form

$$(2x^2 + y)^2 = y^2 + 4y^{m+1}$$

or

$$(2x^2 + y)^2 = y^2(1 + 4y^{m-1}).$$

It follows that $1 + 4y^{m-1}$ is an odd square, say $(2a + 1)^2$. We obtain $y^{m-1} = a(a + 1)$ and since a and $a + 1$ are relatively prime integers, each of them must be the $(m - 1)$ th power of some integers. Clearly, this is possible only if $m = 2$, hence $y = a(a + 1)$. It follows that

$$2x^2 + a(a + 1) = a(a + 1)(2a + 1)$$

hence $x^2 = a^2(a + 1)$. We deduce that $a + 1$ is a square and setting $a + 1 = t^2$ yields $x = t^3 - t$ and $y = t^4 - t^2$.

Problem 3.51 Let m be a positive integer. Find all pairs of integers (x, y) such that

$$x^2(x^2 + y^2) = y^{m+1}.$$

Solution The equation can be written in the equivalent form

$$(2x^2 + y)^2 = y^4 + 4y^{m+1}.$$

Observe that $y^4 + 4y^{m+1}$ cannot be a square for $m = 1$. Indeed, in this case

$$y^4 + 4y^{m+1} = y^4 + 4y^2 = y^2(y^2 + 4)$$

and no squares differ by 4. A similar argument works for $m = 2$.

Now, for $m \geq 3$, we write the equation in the equivalent form

$$(2x^2 + y)^2 = y^4(1 + 4y^{m-3}).$$

As in the previous solution we deduce that $y = a(a + 1)$ for some integer a , then $x = a^3(a + 1)$. It follows that $a = t^2$ for some integer t and the solutions are $x = t^5 + t^3$, $y = t^4 + t^2$.

Problem 3.52 Find all non-negative integers a, b, c, d, n such that

$$a^2 + b^2 + c^2 + d^2 = 7 \cdot 4^n.$$

Solution For $n = 0$, we have $2^2 + 1^2 + 1^2 + 1^2 = 7$, hence $(a, b, c, d) = (2, 1, 1, 1)$ and all permutations. If $n \geq 1$, then $a^2 + b^2 + c^2 + d^2 \equiv 0 \pmod{4}$, hence the numbers have the same parity. We analyze two cases.

(a) The numbers a, b, c, d are odd. We write $a = 2a' + 1$, etc. We obtain

$$4a'(a' + 1) + 4b'(b' + 1) + 4c'(c' + 1) + 4d'(d' + 1) = 4(7 \cdot 4^{n-1} - 1).$$

The left-hand side of the equality is divisible by 8, hence $7 \cdot 4^{n-1} - 1$ must be even. This happens only for $n = 1$. We obtain $a^2 + b^2 + c^2 + d^2 = 28$, with the solutions $(3, 3, 3, 1)$ and $(1, 1, 1, 5)$.

(b) The numbers a, b, c, d are even. Write $a = 2a'$, etc. We obtain

$$a'^2 + b'^2 + c'^2 + d'^2 = 7 \cdot 4^{n-1},$$

so we proceed recursively.

Finally, we obtain the solutions $(2^{n+1}, 2^n, 2^n, 2^n)$, $(3 \cdot 2^n, 3 \cdot 2^n, 3 \cdot 2^n, 2^n)$, $(2^n, 2^n, 2^n, 5 \cdot 2^n)$, and the respective permutations.

Problem 3.53 Show that there are infinitely many systems of positive integers (x, y, z, t) which have no common divisor greater than 1 and such that

$$x^3 + y^3 + z^2 = t^4.$$

Solution Consider the identity

$$(a + 1)^4 - (a - 1)^4 = 8a^3 + 8a.$$

Taking $a = b^3$, with b an even integer gives

$$(b^3 + 1)^4 = (2b^3)^3 + (2b)^3 + ((b^3 - 1)^2)^2.$$

Since b is even, $b^3 + 1$ and $b^3 - 1$ are odd integers. It follows that the numbers $x = 2b^3$, $y = 2b$, $z = (b^3 - 1)^2$ and $t = b^3 + 1$ have no common divisor greater than 1.

Problem 3.54 Let $k \geq 6$ be an integer number. Prove that the system of equations

$$\begin{cases} x_1 + x_2 + \cdots + x_{k-1} = x_k, \\ x_1^3 + x_2^3 + \cdots + x_{k-1}^3 = x_k^3, \end{cases}$$

has infinitely many integral solutions.

Solution Consider the identity

$$(m+1)^3 + (m-1)^3 + (-m)^3 + (-m)^3 = 6m.$$

If n is an arbitrary integer, then $\frac{n-n^3}{6}$ is also an integer since $n - n^3 = -(n-1)n \times (n+1)$ and the product of three consecutive integers is divisible by 6. Setting $m = \frac{n-n^3}{6}$ in the identity above gives

$$\left(\frac{n-n^3}{6} + 1\right)^3 + \left(\frac{n-n^3}{6} - 1\right)^3 + \left(\frac{n^3-n}{6}\right)^3 + \left(\frac{n^3-n}{6}\right)^3 + n^3 = n.$$

On the other hand, we have

$$\left(\frac{n-n^3}{6} + 1\right) + \left(\frac{n-n^3}{6} - 1\right) + \frac{n^3-n}{6} + \frac{n^3-n}{6} + n = n,$$

yielding the following solution for $k=6$: $x_1 = \frac{n-n^3}{6} + 1$, $x_2 = \frac{n-n^3}{6} - 1$, $x_3 = x_4 = \frac{n^3-n}{6}$, $x_5 = x_6 = n$. For $k > 6$ we can take x_1 to x_5 as before, $x_6 = -n$ and $x_i = 0$ for all $i > 6$.

Problem 3.55 Solve in integers the equation

$$x^2 + y^2 = (x-y)^3.$$

Solution If we denote $a = x - y$ and $b = x + y$, the equation rewrites as

$$a^2 + b^2 = 2a^3,$$

or

$$2a - 1 = \frac{b^2}{a^2}.$$

We see that $2a - 1$ is the square of a rational number, hence it is the square of an (odd) integer. Let $2a - 1 = (2n + 1)^2$. It follows that $a = 2n^2 + 2n + 1$ and $b = a(2n + 1) = (2n + 1)(2n^2 + 2n + 1)$. Finally, we obtain

$$x = 2n^3 + 4n^2 + 3n + 1, \quad y = 2n^3 + 2n^2 + n,$$

where n is an arbitrary integer number.

Problem 3.56 Let a and b be positive integers. Prove that if the equation

$$ax^2 - by^2 = 1$$

has a solution in positive integers, then it has infinitely many solutions.

Solution Factor the left-hand side to obtain

$$(x\sqrt{a} - y\sqrt{b})(x\sqrt{a} + y\sqrt{b}) = 1.$$

Cubing both sides yields

$$\begin{aligned} &((x^3a + 3xy^2b)\sqrt{a} - (3x^2ya + y^3b)\sqrt{b})((x^3a + 3xy^2b)\sqrt{a} \\ &\quad + (3x^2ya + y^3b)\sqrt{b}) = 1. \end{aligned}$$

Multiplying out, we obtain

$$a(x^3a + 3xy^2b)^2 - b(3x^2ya + y^3b)^2 = 1.$$

Therefore, if (x_1, y_1) is a solution of the equation, so is (x_2, y_2) , with $x_2 = x_1^3a + 3x_1y_1^2b$, and $y_2 = 3x_1^2y_1a + y_1^3b$. Clearly, $x_2 > x_1$ and $y_2 > y_1$. Continuing in this way we obtain infinitely many solutions in positive integers.

Problem 3.57 Prove that the equation

$$\frac{x+1}{y} + \frac{y+1}{x} = 4$$

has infinitely many solutions in positive integers.

Solution Suppose that the equation has a solution (x_1, y_1) with $x_1 \leq y_1$. Clearing denominators, we can write the equation under the form

$$x^2 - (4y - 1)x + y^2 + y = 0,$$

that is, a quadratic in x . One of the roots is x_1 , therefore, by Vieta's theorem, the second one is $4y_1 - 1 - x_1$. Observe that $4y_1 - 1 - x_1 \geq 4x_1 - 1 - x_1 = 3x_1 - 1 \geq 2x_1 > 0$, hence $4y_1 - 1 - x_1$ is a positive integer.

It follows that $(4y_1 - 1 - x_1, y_1)$ is another solution of the system. Because the equation is symmetric, we obtain that $(x_2, y_2) = (y_1, 4y_1 - 1 - x_1)$ is also a solution. To end the proof, observe that $x_2 + y_2 = 5y_1 - 1 - x_1 > x_1 + y_1$ and that $(1, 1)$ is a solution. Thus, we can generate infinitely many solutions:

$$(1, 1) \rightarrow (1, 2) \rightarrow (2, 6) \rightarrow (6, 21) \rightarrow \cdots$$

Problem 3.58 Prove that the equation

$$x^3 + y^3 - 2z^3 = 6(x + y + 2z)$$

has infinitely many solutions in positive integers.

Solution Observe that

$$(n + 1)^3 + (n - 1)^3 - 2n^3 = 6n,$$

and

$$(n + 1) + (n - 1) + 2n = 4n.$$

Taking $x = 2(n + 1)$, $y = 2(n - 1)$, and $z = 2n$, we see that

$$x^3 + y^3 - 2z^3 = 48n,$$

and

$$6(x + y + 2z) = 48n.$$

Thus, the triples $(x, y, z) = (2(n + 1), 2(n - 1), 2n)$ are solutions in positive integers for all integers $n > 1$.

6.6 Equations with No Solutions

Problem 3.62 Prove that the equation

$$4xy - x - y = z^2$$

has no positive integer solutions.

Solution We write the equation in the equivalent form

$$(4x - 1)(4y - 1) = 4z^2 + 1.$$

Let p be a prime divisor of $4x - 1$. Then

$$4z^2 + 1 \equiv 0 \pmod{p}$$

or

$$(2z)^2 \equiv -1 \pmod{p}.$$

On the other hand, Fermat's theorem yields

$$(2z)^{p-1} \equiv 1 \pmod{p}$$

hence

$$(2z)^{p-1} \equiv (2z^2)^{\frac{p-1}{2}} \equiv (-1)^{\frac{p-1}{2}} \equiv 1 \pmod{p}.$$

This implies that $p \equiv 1 \pmod{4}$. It follows that all prime divisors of $4x - 1$ are congruent to 1 modulo 4, hence $4x - 1 \equiv 1 \pmod{4}$, a contradiction.

Problem 3.63 Prove that the equation

$$6(6a^2 + 3b^2 + c^2) = 5d^2$$

has no solution in non-zero integers.

Solution We can assume that $\gcd(a, b, c, d) = 1$, otherwise we simplify the equation with a suitable integer. Clearly, d is divisible by 6, so let $d = 6m$. We obtain

$$6a^2 + 3b^2 + c^2 = 30m^2,$$

hence c is divisible by 3. Replacing $c = 3n$ in the equation yields

$$2a^2 + b^2 + 3n^2 = 10m^2.$$

If b and n are odd, then $b^2 \equiv 1 \pmod{8}$ and $3n^2 \equiv 3 \pmod{8}$. Because $2a^2 \equiv 0$ or $2 \pmod{8}$ and $10m^2 \equiv 0$ or $2 \pmod{8}$ this leads to a contradiction. Hence b and n must be even and from the initial equation we deduce that a is also even. This contradicts the assumption that $\gcd(a, b, c, d) = 1$.

Problem 3.64 Prove that the system of equations

$$\begin{cases} x^2 + 6y^2 = z^2, \\ 6x^2 + y^2 = t^2 \end{cases}$$

has no positive integer solutions.

Solution As in the previous solution, we can assume that $\gcd(x, y, z, t) = 1$. Adding up the equations yields

$$7(x^2 + y^2) = z^2 + t^2.$$

The square residues modulo 7 are 0, 1, 2, and 4. It is not difficult to see that the only pair of residues which add up to 0 modulo 7 is (0, 0), hence z and t are divisible by 7. Setting $z = 7z_1$ and $t = 7t_1$ yields

$$7(x^2 + y^2) = 49(z_1^2 + t_1^2)$$

or

$$x^2 + y^2 = 7(z_1^2 + t_1^2).$$

It follows that x and y are also divisible by 7, contradicting the fact that $\gcd(x, y, z, t) = 1$.

Problem 3.65 Let k and n be positive integers, with $n > 2$. Prove that the equation

$$x^n - y^n = 2^k$$

has no positive integer solutions.

Solution We may assume x and y are odd, otherwise dividing both x and y by 2 yields a smaller solution. If $n = 2m$ ($m \geq 2$) is even, then we factor to get $(x^m - y^m)(x^m + y^m) = 2^k$. Hence both factors are powers of 2, say $x^m - y^m = 2^r$ and $x^m + y^m = 2^s$, with $s > r$. Solving gives $x^m = 2^{s-1} + 2^{r-1}$ and $y^m = 2^{s-1} - 2^{r-1}$. Since x^m and y^m are odd integers, this forces $r = 1$. But then x^m and y^m are two m th powers which differ by 2, a contradiction. If n is odd, then we factor as

$$(x - y)(x^{n-1} + x^{n-2}y + \cdots + y^{n-1}) = 2^k.$$

The second factor is odd since n is odd and each of the n terms is odd.

Hence it must be 1, which is again a contradiction.

Problem 3.66 Prove that the equation

$$\frac{x^{2000} - 1}{x - 1} = y^2$$

has no positive integer solutions.

Solution Observe that

$$\frac{x^{2000} - 1}{x - 1} = (x^{1000} + 1)(x^{500} + 1)\frac{x^{500} - 1}{x - 1}.$$

Setting

$$a = x^{1000} + 1,$$

$$b = x^{500} + 1,$$

$$c = \frac{x^{500} - 1}{x - 1},$$

we see that b and c divide $a - 2$ and c divides $b - 2$. It follows that the greatest common divisor of any two of a, b, c is at most 2. The product abc is a square only if a, b, c are squares or doubles of squares. It is not difficult to see that a and b cannot be squares, hence they are doubles of squares. This implies that

$$4ab = 4x^{1500} + 4x^{1000} + 4x^{500} + 4$$

is a square. But this is impossible, since a short computation shows that

$$4x^{1500} + 4x^{1000} + 4x^{500} + 4 > (2x^{750} + x^{250})^2$$

and

$$4x^{1500} + 4x^{1000} + 4x^{500} + 4 < (2x^{750} + x^{250} + 1)^2.$$

Problem 3.67 Prove that the equation

$$4(x_1^4 + x_2^4 + \cdots + x_{14}^4) = 7(x_1^3 + x_2^3 + \cdots + x_{14}^3)$$

has no solution in positive integers.

Solution Suppose, by way of contradiction, that such a solution exists. Then

$$\sum_{k=1}^{14} \left(x_k^4 - \frac{7}{4}x_k^3 \right) = 0.$$

Observe that

$$\begin{aligned} \sum (x_k - 1)^4 &= \sum (x_k^4 - 4x_k^3 + 6x_k^2 - 4x_k + 1) \\ &= \sum \left(x_k^4 - \frac{7}{4}x_k^3 - \frac{9}{4}x_k^3 + 6x_k^2 - 4x_k + 1 \right) \\ &= \sum \left(-\frac{9}{4}x_k^3 + 6x_k^2 - 4x_k + 1 \right). \end{aligned}$$

Since

$$-\frac{9}{4}x_k^3 + 6x_k^2 - 4x_k = -x_k \left(\frac{3}{2}x_k - 2 \right)^2 \leq 0$$

we obtain

$$\sum (x_k - 1)^4 \leq 14.$$

This inequality implies that each x_k is equal to either 1 or 2. Now, suppose x of the numbers $x_1, \dots, x_{14}$ are equal to 1 and y of them are equal to 2. Then $x + y = 14$ and the original equation gives

$$4(x + 16y) = 7(x + 8y).$$

We obtain $x = \frac{112}{11}$ and $y = \frac{42}{11}$, a contradiction.

Problem 3.68 Prove that the equation

$$x^2 + y^2 + z^2 = 2011^{2011} + 2012$$

has no solution in integers.

Solution We begin by noticing that a square can only equal 0, 1, or 4 modulo 8. Let us check the right-hand side modulo 8. We have

$$2011 \equiv 3 \pmod{8},$$

hence

$$2011^{2011} \equiv 3^{2011} \equiv (3^2)^{1005} \cdot 3 \equiv 3 \pmod{8},$$

and since

$$2012 \equiv 4 \pmod{8},$$

it follows that

$$2011^{2011} + 2012 \equiv 7 \pmod{8}.$$

Finally, observe that three (not necessarily distinct) numbers from the set $\{0, 1, 4\}$ cannot add to 7 (mod 8), so the equation has no solutions in integers.

Problem 3.69 Prove that the system

$$x^6 + x^3 + x^3y + y = 147^{157},$$

$$x^3 + x^3y + y^2 + y + z^9 = 157^{147}$$

has no solution in integers x , y , and z .

Solution Adding the equations yields

$$x^6 + y^2 + 2x^3y + 2x^3 + 2y + z^9 = 147^{157} + 157^{147}.$$

The first five terms in the left-hand side suggest the expansion of a square, so add 1 to both sides to obtain

$$(x^3 + y + 1)^2 + z^9 = 147^{157} + 157^{147} + 1.$$

We will check both sides of the equation modulo 19. By Fermat's little theorem, if z is not divisible by 19, then $z^{18} \equiv 1 \pmod{19}$, and it follows that $z^9 \equiv \pm 1 \pmod{19}$. On the other hand, the possible remainders of a square modulo 19 are 0, 1, 4, 5, 6, 7, 9, 11, 16, and 17. Therefore the left-hand side can take any value modulo 19 except for 13 and 14.

For the right-hand side, we have (all congruences are mod 19)

$$\begin{aligned} 147^{157} &\equiv 14^{157} \equiv (14^{18})^8 \cdot 14^{13} \equiv 14^{13} \equiv (-5)^{13} \equiv -5^{13} \\ &\equiv -5^{-5} \equiv -4^5 \equiv -1024 \equiv 2. \end{aligned}$$

Similarly,

$$157^{147} \equiv 11 \pmod{19}.$$

It follows that the right-hand side is congruent to 14 modulo 19, hence the equation has no solutions in integers.

Problem 3.70 Prove that the equation

$$x^5 + y^5 + 1 = (x + 2)^5 + (y - 3)^5$$

has no solution in integers.

Solution Assume the contrary. Using Fermat's little theorem and taking both sides modulo 5 we obtain an obvious contradiction.

Observation Why did we choose $p = 19$ to check the equation mod p ? Generally speaking, if in a Diophantine equation we have a term like x^k and $p = 2k + 1$ is a prime number, it is a good idea to check the equation mod p . That is because Fermat's little theorem gives $x^{2k} = (x^k)^2 \equiv 1 \pmod{p}$, if p does not divide x . Hence x^k can only take the values $-1, 0$, and $1 \pmod{p}$.

Problem 3.71 Prove that the equation

$$x^5 = y^2 + 4$$

has no solution in integers.

Solution Taking into account the observation from the previous solution, we will check the equation mod 11. The left-hand side can be $-1, 0$, or 1 . The possible remainders of a square mod 11 are $0, 1, 3, 4, 5, 9$, hence the right-hand side can be $4, 5, 7, 8, 9$, or 2 . Thus, the equality is never possible mod 11.

Problem 3.72 Prove that the equation

$$x^3 - 3xy^2 + y^3 = 2891$$

has no solution in integers.

Solution Observe that $2891 = 7^2 \cdot 59$. If one of x, y is divisible by 7, then so is the other one, and it follows that 7^3 divides 2891, a contradiction. Since $7 \nmid y$, there exists z such that $yz \equiv 1 \pmod{7}$. Multiplying by z^3 and denoting $xz = t$, we obtain

$$t^3 - 3t + 1 \equiv 0 \pmod{7}.$$

6.7 Powers of 2

Problem 3.75 Let n be a positive integer such that $2^n + 1$ is a prime number. Prove that $n = 2^k$, for some integer k .

Solution Suppose that n is not a power of 2. Then it can be written in the form $n = 2^k(2p + 1)$, with $k \geq 0$ and $p \geq 1$. But then we have

$$2^n + 1 = (2^{2^k})^{2^{p+1}} + 1 = (2^{2^k} + 1)((2^{2^k})^{2^p} - (2^{2^k})^{2^{p-1}} + \cdots - 2^{2^k} + 1),$$

hence $2^n + 1$ is not a prime number.

Observation The numbers $F_n = 2^{2^n} + 1$ are called Fermat's numbers. Fermat conjectured that all such numbers are prime, which is true for $n \leq 4$, but Euler proved that $F_5 = 2^{32} + 1$ is divisible by 641. The proof is quite short: notice that $641 = 640 + 1 = 5 \cdot 2^7 + 1$, hence $5 \cdot 2^7 \equiv -1 \pmod{641}$, so that $5^4 \cdot 2^{28} \equiv 1 \pmod{641}$. On the other hand, $641 = 625 + 16 = 5^4 + 2^4$, so $2^4 \equiv -5^4 \pmod{641}$. Multiplying these two congruencies, we obtain $5^4 \cdot 2^{32} \equiv -5^4 \pmod{641}$, hence $2^{32} \equiv -1 \pmod{641}$.

Problem 3.76 Let n be a positive integer such that $2^n - 1$ is a prime number. Prove that n is a prime number.

Solution If n is not a prime number, then $n = ab$, for some positive integers $a, b > 1$. We obtain

$$2^n - 1 = 2^{ab} - 1 = (2^a)^b - 1 = (2^a - 1)((2^a)^{b-1} + (2^a)^{b-2} + \cdots + 2^a + 1),$$

and this factorization shows that $2^n - 1$ is not a prime number.

Problem 3.77 Prove that the number $A = 2^{1992} - 1$ can be written as a product of 6 integers greater than 2^{248} .

Solution It is again an exercise in factorization:

$$\begin{aligned} A &= 2^{1992} - 1 = 2^{249 \cdot 8} - 1 = (2^{249})^8 - 1 \\ &= (2^{249} - 1)(2^{249} + 1)((2^{249})^2 + 1)((2^{249})^4 + 1). \end{aligned}$$

Now, observe that

$$\begin{aligned} (2^{249})^2 + 1 &= (2^{249})^2 + 2 \cdot 2^{249} + 1 - 2^{250} \\ &= (2^{249} + 1)^2 - (2^{125})^2 = (2^{249} - 2^{125} + 1)(2^{249} + 2^{125} + 1), \end{aligned}$$

and

$$\begin{aligned} (2^{249})^4 + 1 &= 2^{996} + 1 = (2^{332})^3 + 1 \\ &= (2^{332} + 1)(2^{664} - 2^{332} + 1). \end{aligned}$$

Thus, the six integers are $2^{249} - 1$, $2^{249} + 1$, $2^{249} - 2^{125} + 1$, $2^{249} + 2^{125} + 1$, $2^{332} + 1$ and $2^{664} - 2^{332} + 1$. It is not difficult to see that all six are greater than 2^{248} .

Problem 3.78 Determine the remainder of $3^{2^n} - 1$ when divided by 2^{n+3} .

Solution Observe that after we use n times the identity

$$x^2 - 1 = (x - 1)(x + 1),$$

we obtain

$$3^{2^n} - 1 = (3 - 1)(3 + 1)(3^2 + 1)(3^{2^2} + 1) \cdots (3^{2^{n-1}} + 1).$$

Now, each of the numbers $3^2 + 1, 3^{2^2} + 1, \dots, 3^{2^{n-1}} + 1$ is divisible by 2 but not by 4. Indeed, $3 \equiv -1 \pmod{4}$, so $3^{2^k} \equiv (-1)^{2^k} \equiv 1 \pmod{4}$ and it follows that $3^{2^k} + 1 \equiv 2 \pmod{4}$. We deduce that there exists an odd integer $2m + 1$ such that

$$(3^2 + 1)(3^{2^2} + 1) \cdots (3^{2^{n-1}} + 1) = 2^{n-1}(2m + 1).$$

Then

$$3^{2^n} - 1 = 2 \cdot 4 \cdot 2^{n-1}(2m + 1) = m \cdot 2^{n+3} + 2^{n+2},$$

and this shows that the requested remainder is 2^{n+2} .

Problem 3.79 Prove that for each n , there exists a number A_n , divisible by 2^n , whose decimal representation contains n digits, each of them equal to 1 or 2.

Solution We prove the assertion by induction on n . For $n = 1$, take $A_1 = 2$; for $n = 2$, take $A_2 = 12$. Now, suppose there exists A_n , divisible by 2^n , whose decimal representation contains n digits, each of them equal to 1 or 2.

If 2^{n+1} divides A_n , then A_{n+1} is obtained by adding the digit 2 at the beginning of A_n . Thus,

$$A_{n+1} = 2 \cdot 10^n + A_n = 2^{n+1} \cdot 5^n + A_n,$$

and we see that this number has $n + 1$ digits 1 or 2 and it is divisible by 2^{n+1} .

If 2^{n+1} does not divide A_n , then $A_n = 2^n k$ for some odd integer k . In this case, we add the digit 1 at the beginning of A_n . It follows that

$$A_{n+1} = 10^n + A_n = 2^n \cdot 5^n + 2^n \cdot k = 2^n(5^n + k).$$

The claim is proved by observing that since k is odd, $5^n + k$ is even, thus A_{n+1} is divisible by 2^{n+1} .

Observation We can prove that the number A_n is unique. Indeed, suppose B_n is another number with the enounced properties. Then $A_n - B_n$ is divisible by 2^n , hence they have the same last digit. Let A_{n-1} and B_{n-1} be the numbers obtained by discarding the last digit of A_n and B_n . Then $A_n - B_n = 10(A_{n-1} - B_{n-1})$, and we deduce that $A_{n-1} - B_{n-1}$ is divisible by 2^{n-1} , hence, again, they have the same last digit. Repeating this argument, we finally deduce that $A_n = B_n$. We can see that we

did not use the fact that A_n and B_n are divisible by 2^n , but only that their difference is divisible by 2^n . This shows that the 2^n numbers with n digits equal to 1 or 2 give different remainders when divided by 2^n . Finally, we observe that the digits 1 and 2 from the enounce can be replaced with any two other non-zero digits with different parities.

Problem 3.80 Using only the digits 1 and 2, one writes down numbers with 2^n digits such that the digits of every two of them differ in at least 2^{n-1} places. Prove that no more than 2^{n+1} such numbers exist.

Solution Let us suppose that $2^{n+1} + 1$ such numbers exist. From these, at least $2^n + 1$ have the same last digit. Denote by A the set of these numbers. For $a, b \in A$, let $c(a, b)$ be the number of digit coincidences. Thus, from the enounce it follows that $c(a, b) \leq 2^{n-1}$, for every a and b . Let N the total number of coincidences for all numbers in A . Then

$$N \leq 2^{n-1} \cdot \binom{2^n + 1}{2} = 2^{3n-2} + 2^{2n-2}.$$

On the other hand, if we arrange the numbers of A in a table with $2^n + 1$ rows and 2^n columns, we count in the last column $\binom{2^n + 1}{2}$ coincidences and in each of the remaining $2^n - 1$ columns at least $2^{2(n-1)}$ coincidences. Indeed, if on some column we have $2^{n-1} - k$ digits of one type and $2^{n-1} + k + 1$ digits of the other type, then the number of coincidences equals

$$\binom{2^{n-1} - k}{2} + \binom{2^{n-1} + k + 1}{2} = 2^{2(n-1)} + k^2 + k \geq 2^{2(n-1)}.$$

We conclude that

$$N \geq \binom{2^n + 1}{2} + (2^n - 1) \cdot 2^{2(n-1)} = 2^{3n-2} + 2^{2n-2} + 2^{n-1}.$$

which is a contradiction.

Observation It can be shown that 2^{n+1} numbers with the required properties exist. We prove this inductively. For $n = 1$, take the numbers 11, 12, 21 and 22, which clearly satisfy the conditions. Suppose there exists a set S_n with 2^{n+1} numbers having 2^n digits such that every two of them differ in at least 2^{n-1} places. We construct a set S_{n+1} with 2^{n+2} numbers having 2^{n+1} digits generating from each element of S_n two elements of S_{n+1} as follows: if $a = \overline{a_1 a_2 \dots a_n} \in S_n$, then in S_{n+1} we put $b = \overline{a_1 a_2 \dots a_n a_1 a_2 \dots a_n}$ and $c = \overline{a_1 a_2 \dots a_n a'_1 a'_2 \dots a'_n}$, where $a'_k = 1$ if $a_k = 2$ and $a'_k = 2$ if $a_k = 1$. For instance, if $S_2 = \{11, 12, 21, 22\}$, then $S_3 = \{1111, 1212, 2121, 2222, 1122, 1221, 2112, 2211\}$. It is not difficult to check that the set thus obtained has the required properties.

Problem 3.81 Does there exist a natural number N which is a power of 2 whose digits (in the decimal representation) can be permuted to form a different power of 2?

Solution The answer is negative. Indeed, suppose such N exists and let N' another power of 2 obtained by rearranging the digits of N . We can assume that $N < N'$. Since N and N' have the same number of digits, we must have $N' = 2N$, or $N' = 4N$ or $N' = 8N$. It results that

$$N' - N \in \{N, 3N, 7N\}.$$

We get a contradiction from the following.

Lemma Let $n = \overline{a_k a_{k-1} \dots a_1 a_0}$ be a positive integer and

$$s(n) = a_k + a_{k-1} + \dots + a_1 + a_0$$

the sum of its digits. Then the difference $n - s(n)$ is divisible by 9.

Proof We have

$$\begin{aligned} n - s(n) &= a_k \cdot 10^k + a_{k-1} \cdot 10^{k-1} + \dots + a_1 \cdot 10 + a_0 - a_k - a_{k-1} - \dots \\ &\quad - a_1 - a_0 \\ &= a_k(10^k - 1) + a_{k-1}(10^{k-1} - 1) + \dots + a_1(10 - 1), \end{aligned}$$

and the conclusion follows by noticing that every number of the form $10^p - 1$ is divisible by 9.

Returning to our problem, we see that since N and N' have the same digits, $s(N) = s(N')$, thus $N' - N$ must be divisible by 9. This is impossible, because $N' - N \in \{N, 3N, 7N\}$ and none of the numbers $N, 3N, 7N$ is divisible by 9. $\square$

Problem 3.82 For a positive integer N , let $s(N)$ the sum of its digits, in the decimal representation. Prove that there are infinitely many n for which $s(2^n) > s(2^{n+1})$.

Solution We use again the above lemma. Suppose, by way of contradiction, that there exist finitely many n for which $s(2^n) > s(2^{n+1})$. Then there exists m such that for every $n > m$, $s(2^n) \leq s(2^{n+1})$. Since $s(2^n) = s(2^{n+1})$ if and only if $2^{n+1} - 2^n = 2^n$ is divisible by 9, we deduce that the sequence $s(2^n)$ is strictly increasing for $n > m$. Moreover, since the remainders of the numbers 2^n divided by 9 are 2, 4, 8, 7, 5, 1 and repeat periodically after 6 steps, we deduce that

$$s(2^{n+6}) \geq s(2^n) + 2 + 4 + 8 + 7 + 5 + 1 = s(2^n) + 27$$

and then, inductively, that

$$s(2^{n+6k}) \geq s(2^n) + 27k,$$

for $n > m$ and all positive integers k .

On the other hand, $2^3 < 10$, so $2^{n+6k} < 10^{\frac{n}{3}+2k}$ and this shows that the number 2^{n+6k} has at most $\frac{n}{3} + 2k$ digits in its decimal representation. It follows that

$$s(2^{n+6k}) \leq 9\left(\frac{n}{3} + 2k\right) = 3n + 18k.$$

Combining the two estimates of $s(2^{n+6k})$, we deduce

$$s(2^n) + 27k \leq 3n + 18k,$$

for every positive integer k . This is a contradiction.

Problem 3.83 Find all integers of the form 2^n (where n is a natural number) such that after deleting the first digit of its decimal representation we again get a power of 2.

Solution Suppose 2^m is obtained after deleting the first digit (equal to a) of the decimal representation of 2^n . We have then $2^n = 10^k a + 2^m$, for some integer k , hence $2^{n-m} - 1$ is divisible by 5. Checking the remainders of the powers of 2 divided by 5, it results that $2^{n-m} - 1$ is divisible by 5 if and only if $n - m = 4t$, for some positive integer t . But then

$$10^k a = 2^m (2^{4t} - 1) = 2^m (2^{2t} + 1)(2^{2t} - 1) = 2^m (2^{2t} + 1)(2^t + 1)(2^t - 1).$$

Observe that $2^{2t} + 1$ and $2^{2t} - 1$ are odd integers differing by 2, therefore are relatively prime. The same applies to $2^t + 1$ and $2^t - 1$, hence $2^{2t} + 1$, $2^t + 1$ and $2^t - 1$ are all odd, pairwise prime integers. If $t > 1$, then each of the three numbers has an odd prime divisor, but this is impossible, since $10^k a$ is divisible by 5 and at most one of the numbers 3 and 7 (if any of them divides a). Consequently, $t = 1$, hence $10^k a = 2^m \cdot 3 \cdot 5$, which leads to $k = 1$ and $a = 2^{m-1} \cdot 3$. The only possible cases are $m = 1$ and $m = 2$, so the solutions to the problem are $2^5 = 32$ and $2^6 = 64$.

Problem 3.84 Let $a_0 = 0$, $a_1 = 1$ and, for $n \geq 2$, $a_n = 2a_{n-1} + a_{n-2}$. Prove that a_n is divisible by 2^k if and only if n is divisible by 2^k .

Solution Using the standard algorithm for recurrence relations, we obtain

$$a_n = \frac{1}{2\sqrt{2}}[(1 + \sqrt{2})^n - (1 - \sqrt{2})^n],$$

for every positive integer n . If we define

$$b_n = \frac{1}{2}[(1 + \sqrt{2})^n + (1 - \sqrt{2})^n],$$

we observe that b_n satisfies the same recurrence relation, and since $b_0 = b_1 = 1$, all b_n are positive integers.

We have

$$b_n + a_n\sqrt{2} = (1 + \sqrt{2})^n$$

and

$$b_n - a_n\sqrt{2} = (1 - \sqrt{2})^n.$$

Multiplying these equalities we obtain $b_n^2 - 2a_n^2 = (-1)^n$, hence b_n is odd for each n .

Now, we prove the claim by induction on k . For $k = 0$ we have to prove that a_n is odd if and only if n is odd. We have

$$2a_n^2 = b_n^2 - (-1)^n$$

and $b_n = 2m + 1$, for some integer m , hence

$$a_n^2 = 2(m^2 + m) + \frac{1 - (-1)^n}{2}.$$

It follows that a_n is odd if and only if $1 - (-1)^n = 2$, that is, n is odd. The inductive step follows from the equality

$$a_{2n} = 2a_nb_n,$$

which is obtained observing that

$$b_{2n} + a_{2n}\sqrt{2} = (1 + \sqrt{2})^{2n} = (b_n + a_n\sqrt{2})^2 = b_n^2 + 2a_n^2 + 2a_nb_n\sqrt{2}.$$

Problem 3.85 If $A = \{a_1, a_2, \dots, a_p\}$ is a set of real numbers such that $a_1 > a_2 > \dots > a_p$, we define

$$s(A) = \sum_{k=1}^p (-1)^{k-1} a_k.$$

Let M be a set of n positive integers. Prove that $\sum_{A \subseteq M} s(A)$ is divisible by 2^{n-1} .

Solution Let $M = \{a_1, a_2, \dots, a_n\}$. We can assume that

$$a_1 > a_2 > \dots > a_n.$$

Let $A \subseteq M - \{a_1\}$, $A = \{a_{i_1}, a_{i_2}, \dots, a_{i_s}\}$, with $a_{i_1} > a_{i_2} > \dots > a_{i_s}$, and $A' = A \cup \{a_1\}$. Then

$$a_1 > a_{i_1} > a_{i_2} > \dots > a_{i_s}$$

and we have

$$s(A) + s(A') = a_{i_1} - a_{i_2} + \dots + (-1)^{s-1} a_{i_s} + a_1 - a_{i_1} + a_{i_2} - \dots + (-1)^s a_{i_s} = a_1.$$

Now, matching all the 2^{n-1} subsets A of the set $M - \{a_1\}$ with the corresponding subsets $A' = A \cup \{a_1\}$, we find

$$\sum_{A \subseteq M} s(A) = 2^{n-1} a_1,$$

and the claim is proved.

Problem 3.86 Find all positive integers a, b , such that the product

$$(a + b^2)(b + a^2)$$

is a power of 2.

Solution We begin by noticing that a and b must have the same parity. Let $a + b^2 = 2^m$ and $b + a^2 = 2^n$, and assume that $m \geq n$. Then $a + b^2 \geq b + a^2$, or $b^2 - b \geq a^2 - a$, which implies $b \geq a$. Subtracting the two equalities yields

$$(b - a)(a + b - 1) = 2^m - 2^n = 2^n(2^{m-n} - 1).$$

Because $a + b - 1$ is odd, it follows that 2^n divides $b - a$. Let $b - a = 2^n c$, for some positive integer c . Then $b = 2^n c + a = 2^n - a^2$, therefore $a + a^2 = 2^n(1 - c)$, which implies $c = 0$, hence $a = b$.

Finally, we deduce that $a(a + 1)$ is a power of 2, and this is possible only for $a = 1$.

Problem 3.87 Let $f(x) = 4^x + 6^x + 9^x$. Prove that if m and n are positive integers, then $f(2^m)$ divides $f(2^n)$ whenever $m \leq n$.

Solution Define $g(x) = 4^x - 6^x + 9^x$. From the identity

$$(a^2 + ab + b^2)(a^2 - ab + b^2) = a^4 + a^2b^2 + b^4$$

taking $a = 2$ and $b = 3$, we deduce that

$$f(x)g(x) = f(2x).$$

Iterating this, we get

$$f(x)g(x)g(2x) \cdots g(2^{k-1}x) = f(2^k x),$$

for all $k \geq 2$.

Now, suppose $m \leq n$. Then

$$f(2^m)g(2^m)g(2^{m+1}) \cdots g(2^{n-1}) = f(2^n),$$

hence $f(2^m)$ divides $f(2^n)$.

Problem 3.88 Show that, for any fixed integer $n \geq 1$, the sequence

$$2, 2^2, 2^{2^2}, 2^{2^{2^2}}, \dots \pmod{n}$$

is eventually constant.

Solution For a more comfortable notation, define $x_0 = 1$ and $x_{m+1} = 2^{x_m}$, for $m \geq 0$. We have to prove that the sequence $(x_m)_{m \geq 0}$ is eventually constant mod n .

We will prove by induction on n the following statement: $x_k \equiv x_{k+1} \pmod{n}$, for all $k \geq n$.

For $n = 1$ there is nothing to prove. Assume that the statement is true for all numbers less than n . If $n = 2^a \cdot b$, with odd b , it suffices to prove that $x_k \equiv x_{k+1} \pmod{2^a}$, and $x_k \equiv x_{k+1} \pmod{b}$, for all $k \geq n$.

It is not difficult to prove inductively that $x_n > n$. Therefore, if $k \geq n$, we have $x_k \equiv 0 \pmod{2^a}$ (x_k is a power of 2 greater than n , thus greater than 2^a), whence $x_k \equiv x_{k+1} \pmod{2^a}$.

For the second congruence, observe that $x_k \equiv x_{k+1} \pmod{b}$ is equivalent to $2^{x_{k-1}} \equiv 2^{x_k} \pmod{b}$, or $2^{x_k - x_{k-1}} \equiv 1 \pmod{b}$. The latter is true whenever $x_{k-1} \equiv x_k \pmod{\phi(b)}$ (ϕ is Euler's totient function), but this follows from the induction hypothesis, since $\phi(b) \leq b - 1 \leq n - 1$.

6.8 Progressions

Problem 3.92 Partition the set of positive integers into two subsets such that neither of them contains a non-constant arithmetical progression.

Solution Partition the set $\{1, 2, 3, \dots\}$ in the following way:

$$\begin{array}{cccccccccc} 1 & & & 4 & 5 & 6 & & & & \dots \\ & 2 & 3 & & & & 7 & 8 & 9 & 10 & \dots \end{array}$$

None of the sets

$$A = \{1, 4, 5, 6, 11, 12, 13, 14, 15, \dots\}$$

or

$$B = \{2, 3, 7, 8, 9, 10, 16, 17, 18, 19, 20, 21, 22, \dots\}$$

contains a non-constant arithmetical progression. Indeed, if such a progression is contained in one of the sets, let r be its common difference. But in both sets we can find a “gap” of more than r consecutive integers, a contradiction.

Problem 3.93 Prove that among the terms of the progression $3, 7, 11, \dots$ there are infinitely many prime numbers.

Solution Suppose the contrary and let p be the greatest prime number in the given progression. Consider the number

$$n = 4p! - 1.$$

It is not difficult to see that it is a term of the progression (in fact, the given progression contains all positive integers of the form $4k - 1$). Thus n must be composite, since $n > p$. Observe that n is not divisible by any prime of the form $4k - 1$ (all these are factors in $p!$), hence all the prime factors of n are of the form $4k + 1$. The product of several factors of the form $4k + 1$ is again of the form $4k + 1$, hence $n = 4k + 1$, for some k . This is a contradiction.

Problem 3.94 Does there exist an (infinite) non-constant arithmetical progression whose terms are all prime numbers?

Solution The answer is negative. Indeed, if such progression exists, denote its common difference by r , and consider the consecutive r integers

$$(r + 1)! + 2, (r + 1)! + 3, \dots, (r + 1)! + (r + 1).$$

Each of them is a composite number, but since the progression has the common difference r , one out of any r consecutive integers must be a term of the progression. This is a contradiction.

Problem 3.95 Consider an arithmetical progression of positive integers. Prove that one can find infinitely many terms the sum of whose decimal digits is the same.

Solution Let $(a_n)_{n \geq 1}$ be the progression and denote by r its common difference. Suppose the number a_1 has d digits (in its decimal representation). Then for all $k > d$ the digits sum of the number

$$a_1 + 10^k r$$

is the same.

Problem 3.96 The set of positive integers is partitioned into n arithmetical progressions, with common differences $r_1, r_2, \dots, r_n$. Prove that

$$\frac{1}{r_1} + \frac{1}{r_2} + \dots + \frac{1}{r_n} = 1.$$

Solution Let $a_k = a_1 + (k - 1)r_1$ the progression with common difference r_1 . Let us count how many terms of this sequence are less than or equal to some positive integer N . The inequality $a_k \leq N$ is equivalent to

$$a_1 + (k - 1)r_1 \leq N$$

or

$$k \leq \frac{N}{r_1} - \frac{a}{r_1} + 1.$$

It follows that the number of terms of the first progression belonging to the set $\{1, 2, \dots, N\}$ equals

$$\left\lfloor \frac{N}{r_1} - \frac{a}{r_1} + 1 \right\rfloor.$$

Similarly, we deduce that the number of terms of the progression with common difference r_i belonging to the set $\{1, 2, \dots, N\}$ equals

$$\left\lfloor \frac{N}{r_i} - \frac{a}{r_i} + 1 \right\rfloor.$$

Since the progressions form a partition of the set of positive integers, we must have

$$\sum_{i=1}^n \left\lfloor \frac{N}{r_i} - \frac{a}{r_i} + 1 \right\rfloor = N.$$

Using the inequality $\lfloor x \rfloor \leq x < \lfloor x \rfloor + 1$, we obtain

$$N \leq \sum_{i=1}^n \left(\frac{N}{r_i} - \frac{a}{r_i} + 1 \right) < N + n$$

hence

$$1 \leq \sum_{i=1}^n \frac{1}{r_i} - \frac{1}{N} \sum_{i=1}^n \frac{na}{r_i} + \frac{n}{N} < 1 + \frac{n}{N}$$

and letting $N \rightarrow \infty$ yields the desired result.

Problem 3.97 Prove that for every positive integer n one can find n integers in arithmetical progression, all of them nontrivial powers of some integers, but one cannot find an infinite sequence with this property.

Solution We prove the assertion by induction on n . For $n = 3$, we can consider the numbers 1, 25, 49. Suppose the assertion is true for some n and let $a_i = b_i^{k_i}$, $i = 1, 2, \dots, n$, be the terms of the progression having the common difference d . Let $b = a_n + d$ and let $k = \text{lcm}(k_1, k_2, \dots, k_n)$. Then the $n + 1$ numbers

$$a_1 b^k, a_2 b^k, \dots, a_n b^k, b^{k+1}$$

are in progression and all are power of some integers. Indeed, for all i , $1 \leq i \leq n$, there exists d_i such that $k = k_i d_i$ and we obtain

$$a_i b^k = b_i^{k_i} b^k = b_i^{k_i} b^{k_i d_i} = (b_i b^{d_i})^{k_i},$$

as desired.

For the second part, we need a result from Calculus: if $a, b > 0$ then

$$\lim_{n \rightarrow \infty} \sum_{k=1}^n \frac{1}{ak + b} = +\infty.$$

From this we deduce that if $(a_n)_{n \geq 1}$ is a progression of positive integers, then

$$\lim_{n \rightarrow \infty} \sum_{k=1}^n \frac{1}{a_k} = +\infty.$$

Now suppose that $(a_n)_{n \geq 1}$ is a progression in which all terms are powers of some integers. Let S be the set of all positive integers greater than 1 that are powers of some integers. We will prove that

$$\sum_{a \in S} \frac{1}{a} \leq 1$$

which contradicts the previous result. Indeed, we have

$$\begin{aligned} \sum_{a \in S} \frac{1}{a} &\leq \sum_{n \geq 2} \sum_{k \geq 2} \frac{1}{n^k} = \sum_{n \geq 2} \frac{1}{n^2} \left(1 + \frac{1}{n} + \frac{1}{n^2} + \cdots \right) \\ &= \sum_{n \geq 2} \frac{1}{n^2} \cdot \frac{1}{1 - \frac{1}{n}} = \sum_{n \geq 2} \frac{1}{n(n-1)} = \sum_{n \geq 2} \left(\frac{1}{n-1} - \frac{1}{n} \right) = 1. \end{aligned}$$

Problem 3.98 Prove that for any integer $n, n \geq 3$, there exist n positive integers in arithmetical progression $a_1, a_2, \dots, a_n$ and n positive integers in geometric progression $b_1, b_2, \dots, b_n$, such that

$$b_1 < a_1 < b_2 < a_2 < \cdots < b_n < a_n.$$

Solution Let $m > n^2$ be an integer. We define

$$B_k = \left(1 + \frac{1}{m} \right)^k,$$

for $k = 1, 2, \dots, n$. Observe that for $k \geq 2$

$$B_k > 1 + \frac{k}{m}.$$

For $k \leq n$ we have

$$\begin{aligned} B_k &= 1 + \frac{k}{m} + \frac{k(k-1)}{2!m^2} + \cdots + \frac{k!}{k!m^k} \\ &\leq 1 + \frac{k}{m} + \frac{n(n-1)}{2!m^2} + \cdots + \frac{n(n-1) \cdots (n-k+1)}{k!m^k} \end{aligned}$$

$$\begin{aligned}
&= 1 + \frac{k}{m} + \frac{1}{m} \left(\frac{n(n-1)}{2!m} + \cdots + \frac{n(n-1) \cdots (n-k+1)}{k!m^{k-1}} \right) \\
&< 1 + \frac{k}{m} + \frac{1}{m} \left(\frac{1}{2!} + \frac{1}{3!} + \cdots + \frac{1}{k!} \right) < 1 + \frac{k+1}{m}.
\end{aligned}$$

We have used the fact that $m > n^2$ and the inequalities

$$\frac{1}{2!} + \frac{1}{3!} + \cdots + \frac{1}{k!} < \frac{1}{1 \cdot 2} + \frac{1}{2 \cdot 3} + \cdots + \frac{1}{(k-1) \cdot k} = 1 - \frac{1}{k} < 1.$$

Defining

$$A_k = 1 + \frac{k+1}{n}$$

for $1 \leq k \leq n$, yields

$$B_1 < A_1 < B_2 < A_2 < \cdots < B_n < A_n.$$

In order to obtain progressions with integer terms we define $a_k = nm^n A_k$ and $b_k = nm^n B_k$, for all k , $1 \leq k \leq n$.

Problem 3.99 Let $(a_n)_{n \geq 1}$ be an arithmetic sequence such that a_1^2 , a_2^2 , and a_3^2 are also terms of the sequence. Prove that the terms of this sequence are all integers.

Solution Let d be the common difference. If $d = 0$, then it is not difficult to see that either $a_n = 0$ for all n , or $a_n = 1$ for all n . Suppose that $d \neq 0$, and consider the positive integers m, n, p , such that $a_1^2 = a_1 + md$, $(a_1 + d)^2 = a_1 + nd$, and $(a_1 + 2d)^2 = a_1 + pd$. Subtracting the first equation from the other two yields

$$\begin{cases} 2a_1 + d = n - m, \\ 4a_1 + 4d = p - m \end{cases}$$

and solving for a_1 and d we obtain

$$\begin{aligned}
a_1 &= \frac{1}{4}(4n - 3m - p), \\
d &= \frac{1}{2}(m - 2n + p),
\end{aligned}$$

hence both a_1 and d are rational numbers.

Observe that the equation $a_1^2 = a_1 + md$ can be written as

$$a_1^2 + (2m - 1)a_1 - m(d + 2a_1) = 0,$$

or

$$a_1^2 + (2m - 1)a_1 - m(n - m) = 0,$$

hence a_1 is the root of the polynomial with integer coefficients

$$P(x) = x^2 + (2m - 1)x - m(n - m).$$

By the integer root theorem it follows that a_1 is an integer, hence $d = n - m - 2a_1$ is an integer as well. We conclude that all terms of the sequence are integer numbers.

Problem 3.100 Let $A = \{1, \frac{1}{2}, \frac{1}{3}, \frac{1}{4}, \dots\}$. Prove that for every positive integer $n \geq 3$ the set A contains a non-constant arithmetic sequence of length n , but it does not contain an infinite non-constant arithmetic sequence.

Solution For $n = 3$ we have the almost obvious example

$$\frac{1}{6}, \frac{1}{3}, \frac{1}{2}.$$

Writing this as

$$\frac{1}{6}, \frac{2}{6}, \frac{3}{6}$$

might give us a clue for the general case. Indeed, consider the arithmetic sequence

$$\frac{1}{n!}, \frac{2}{n!}, \dots, \frac{n}{n!}.$$

When we write the fractions in their lowest terms, we see that all belong to A .

For the second part, just observe that every non-constant, infinite arithmetic progression is necessarily an unbounded sequence. Since A is bounded, it cannot contain such a sequence.

Problem 3.101 Let n be a positive integer and let $x_1 \leq x_2 \leq \dots \leq x_n$ be real numbers. Prove that

$$\left(\sum_{i,j=1}^n |x_i - x_j| \right)^2 \leq \frac{2(n^2 - 1)}{3} \sum_{i,j=1}^n (x_i - x_j)^2.$$

Show that the equality holds if and only if $x_1, \dots, x_n$ is an arithmetic sequence.

Solution Suppose the given numbers are the terms of an arithmetic sequence, with common difference d . Then $x_i - x_j = (i - j)d$ and the equality we have to prove becomes

$$\left(\sum_{i,j=1}^n |i - j| \right)^2 = \frac{2(n^2 - 1)}{3} \sum_{i,j=1}^n (i - j)^2.$$

We have

$$\begin{aligned}
 \sum_{i,j=1}^n |i-j| &= \sum_{i=1}^n \sum_{j=1}^n |i-j| = \sum_{i=1}^n \left(\sum_{j=1}^i (i-j) + \sum_{j=i+1}^n (j-i) \right) \\
 &= \sum_{i=1}^n \left(i^2 - \frac{i(i+1)}{2} + \frac{n(n+1)}{2} - \frac{i(i+1)}{2} - i(n-i) \right) \\
 &= \sum_{i=1}^n \left(i^2 - (n+1)i + \frac{n(n+1)}{2} \right) \\
 &= \frac{n(n+1)(2n+1)}{6} - \frac{n(n+1)^2}{2} + \frac{n^2(n+1)}{2} \\
 &= \frac{n(n^2-1)}{3}.
 \end{aligned}$$

On the other hand,

$$\begin{aligned}
 \sum_{i,j=1}^n (i-j)^2 &= \sum_{i=1}^n \left(\sum_{j=1}^n (i^2 - 2ij + j^2) \right) \\
 &= \sum_{i=1}^n \left(ni^2 - in(n+1) + \frac{n(n+1)(2n+1)}{6} \right) \\
 &= \frac{n^2(n+1)(2n+1)}{6} - \frac{n^2(n+1)^2}{2} + \frac{n^2(n+1)(2n+1)}{6} \\
 &= \frac{n^2(n^2-1)}{6}.
 \end{aligned}$$

Thus, the equality to prove is written as

$$\left(\frac{n(n^2-1)}{3} \right)^2 = \frac{2(n^2-1)}{3} \cdot \frac{n^2(n^2-1)}{6},$$

obviously true.

In order to prove the inequality, observe that

$$\begin{aligned}
 \sum_{i,j=1}^n (x_i - x_j)^2 &= \sum_{i=1}^n \sum_{j=1}^n (x_i^2 - 2x_i x_j + x_j^2) \\
 &= \sum_{i=1}^n \left(nx_i^2 - 2x_i \sum_{j=1}^n x_j + \sum_{j=1}^n x_j^2 \right) \\
 &= 2n \sum_{i=1}^n x_i^2 - 2 \left(\sum_{i=1}^n x_i \right)^2.
 \end{aligned}$$

In a similar way and taking into account the ordering of the x_i 's, we obtain

$$\sum_{i,j=1}^n |x_i - x_j| = 2 \sum_{i=1}^n (2i - n - 1)x_i.$$

Thus, the inequality becomes

$$\left(\sum_{i=1}^n (2i - n - 1)x_i \right)^2 \leq \frac{n^2 - 1}{3} \left(n \sum_{i=1}^n x_i^2 - \left(\sum_{i=1}^n x_i \right)^2 \right).$$

The key observation is that we can replace all x_i 's by $x_i + c$, for an arbitrary constant c . Indeed, if we look at the original inequality, we see that the differences $x_i - x_j$ remain unchanged. Therefore, we can choose the constant c such that $\sum_{i=1}^n x_i = 0$. In this way we only have to check that

$$\left(\sum_{i=1}^n (2i - n - 1)x_i \right)^2 \leq \frac{n^2 - 1}{3} \left(n \sum_{i=1}^n x_i^2 \right),$$

which follows easily from Cauchy–Schwarz if we observe that

$$\sum_{i=1}^n (2i - n - 1) = \frac{n(n^2 - 1)}{3}.$$

The equality occurs if there exists d such that $x_i = d(2i - n - 1)$, for all i , hence if the numbers $x_1, x_2, \dots, x_n$ form an arithmetic sequence.

6.9 The Marriage Lemma

Problem 3.104 A deck of cards is arranged, face up, in a 4×13 array. Prove that one can pick a card from each column in such a way as to get one card of each denomination.

Solution Consider the columns as boys and the denominations as girls. A boy is acquainted with a girl if in that column there exists a card of the respective denomination. Now choose k boys. They are acquainted with $4k$ (not necessarily distinct) girls. But each girl appears at most four times, since there are four cards of each denomination. Therefore, the number of distinct girls acquainted to the k boys is at least k , hence Hall's condition holds. The matching between the columns and the denominations show us how to pick the cards.

Problem 3.105 An $n \times n$ table is filled with 0 and 1 so that if we chose randomly n cells (no two of them in the same row or column) then at least one contains 1. Prove that we can find i rows and j columns so that $i + j \geq n + 1$ and their intersection contains only 1's.

Solution Let the rows be the boys and the columns be the girls. A boy is acquainted with a girl if at the intersection of the respective row and column there is a 0. Then the hypothesis simply says that there is no matching between the boys and the girls.

We deduce that Hall's condition is violated, hence we can find i rows such that such that the columns they are acquainted with are at most $i - 1$. But then at the intersections of these i rows and the remaining $j \geq n - i + 1$ columns there are only 1's. The conclusion is obvious.

Problem 3.106 Let X be a finite set and let $\bigsqcup_{i=1}^n X_i = \bigsqcup_{j=1}^n Y_j$ be two disjoint decompositions with all sets X_i 's and Y_j 's having the same size. Prove that there exist distinct elements $x_1, x_2, \dots, x_n$ which are in different sets in both decompositions.

Solution Let us examine an example: $X = \{1, 2, 3, 4, 5, 6, 7, 8, 9\}$ and

$$X = \{1, 2, 3\} \cup \{4, 5, 6\} \cup \{7, 8, 9\} = \{1, 4, 7\} \cup \{2, 3, 6\} \cup \{5, 8, 9\}.$$

We see that 1, 6, and 9 are in different sets in both decompositions.

In the general case, consider the sets X_i as boys and Y_j as girls. We say that X_i is acquainted with Y_j if $X_i \cap Y_j \neq \emptyset$. Suppose that there is a matching between the boys and the girls such that X_i is matched with $Y_{\sigma(i)}$, for each i . Then we can choose $x_i \in X_i \cap Y_{\sigma(i)}$ and we are done.

In order to prove the existence of such a matching, we will show that Hall's condition holds. Suppose that all the sets have m elements and choose k sets X_i . Their union has mk elements (because the sets are disjoint) and therefore there must be at least k corresponding sets Y_j .

Problem 3.107 A set P consists of 2005 distinct prime numbers. Let A be the set of all possible products of 1002 elements of P , and B be the set of all products of 1003 elements of P . Prove the existence of a one-to-one correspondence f from A to B with the property that a divides $f(a)$ for all $a \in A$.

Solution The set A has $\binom{2005}{1002}$ elements and these are the boys. The set B has the same number of elements, since

$$\binom{2005}{1003} = \binom{2005}{1002}$$

and these are the girls. A boy a is acquainted with a girl b if a divides b . We have to prove that there exists a matching between the boys and the girls. For this, observe that each boy is acquainted with exactly 1003 girls, and each girl is acquainted with exactly 1003 boys. The existence of a matching follows from the observation at the end of the solution of Problem 3.103.

Problem 3.108 The entries of a $n \times n$ table are non-negative real numbers such that the numbers in each row and column add up to 1. Prove that one can pick n numbers from distinct rows and columns which are positive.

Solution Again, the rows are the boys and the columns are the girls. We say that a row is acquainted to a column if the entry at their intersection is a positive number. All we have to do is to show that Hall's condition is fulfilled.

Choose k rows and consider the m columns acquainted to them. Color red the cells of the k rows and blue the cells of the m columns. Consequently, the cells at their intersection will be colored violet. It is not difficult to see that the entries in all red cells are zeroes. Adding up the entries of the k rows yields k , hence the entries at the violet cells add up to k as well. Adding up the entries of the m columns yields m , therefore the sum of entries in the violet and blue cells equals m . Clearly, this implies $k \leq m$, so Hall's condition is indeed fulfilled.

Problem 3.109 There are b boys and g girls present at a party, where b and g are positive integers satisfying $g \geq 2b - 1$. Each boy invites a girl for a dance (of course, two different boys must always invite two different girls). Prove that this can be done in such a way that every boy is either dancing with a girl he knows or all the girls he knows are not dancing.

Solution If Hall's condition is fulfilled, then each boy can invite for the dance a girl he knows. Suppose that Hall's condition is violated and thus, we can find k boys, say $b_1, b_2, \dots, b_k$, such that the girls they know are $g_1, g_2, \dots, g_m$, with $m < k$. We choose the maximal k with this property. Now, observe that for the rest of $b - k$ boys and $g - m$ girls, Hall's condition is fulfilled (otherwise the maximality of k is contradicted), hence we can make the $b - k$ boys dance with $b - k$ girls they know. We are left with $g - m - (b - k) \geq 2b - 1 - b + k - m \geq k$ girls and we can make $b_1, b_2, \dots, b_k$ dance with k of these girls.

Problem 3.110 A $m \times n$ array is filled with the numbers $1, 2, \dots, n$, each used exactly m times. Show that one can always permute the numbers within columns to arrange that each row contains every number $1, 2, \dots, n$ exactly once.

Solution Let us show first that we can permute the numbers within columns such that the first row contains every number $1, 2, \dots, n$ exactly once. Let the columns be the boys and let the numbers $1, 2, \dots, n$ be the girls. A boy (column) is acquainted with a girl (number) if that number occurs in the column. Now, consider a set of k columns; they contain km numbers, hence there exist at least k distinct numbers among them. Since Hall's condition is fulfilled, there is a matching between the columns and the numbers $1, 2, \dots, n$. Permuting these numbers to the tops of their respective columns makes the first row contain all n numbers. Finally, a simple inductive argument ends the proof.

Problem 3.111 Some of the AwesomeMath students went on a trip to the beach. There were provided n buses of equal capacities for both the trip to the beach and the ride home, one student in each seat, and there were not enough seats in $n - 1$ buses to fit each student. Every student who left in a bus came back in a bus, but not necessarily the same one.

Prove that there are n students such that any two were on different busses on both rides.

Solution Let the buses be $b_1, b_2, \dots, b_n$. Denote by X_i the set of students traveling in bus b_i to the beach and by Y_i the set of students traveling in bus b_i on the ride home. Let the X_i 's be the boys and the Y_i 's be the girls. We say that a boy X_i is acquainted with the girl Y_j if $X_i \cap Y_j \neq \emptyset$. Now consider a set of k boys $X_1, X_2, \dots, X_k$. If the set of girls acquainted with them has less than k elements then the students in $X_1 \cup X_2 \cup \dots \cup X_k$ fit in $k - 1$ buses, hence all students fit in $n - 1$ buses, contradicting the hypothesis. Therefore there is a matching between the two sets. If X_i is matched with $Y_{\sigma(i)}$, then we can pick a student from each $X_i \cap Y_{\sigma(i)}$ and we are done.

Mathematical Olympiad Treasures

Andreescu, T.; Enescu, B.

2012, VIII, 253 p., Hardcover

ISBN: 978-0-8176-8252-1

A product of Birkhäuser Basel