Some Elementary Problems (Solved and Unsolved) in Number Theory and Geometry

Paul Erdös
The Hungarian Academy of Science and Technion, Haifa

Dedicated to the memory of Prof. J. Gillis

Mathematics is full of unsolved problems. Many well educated people believe that mathematics is really a closed subject where everything is already known. Perhaps it would be good to explain already early in school how false this is. Let me illustrate this by the following example. At the international congress in Cambridge, England in 1912[1]. Landau gave the talk in analytic number theory and he stated first of all four problems "Unangreifbar beim heutigen Stand der Wissenschaften"– unattackable by the present state of science (Landau talked in German). The four problems which every baby can understand are still unattackable. Here they are: (1) Every even number > 2 is the sum of two primes. (2) There are infinitely many prime twins i.e. primes whose difference is 2. (3) between two consecutive squares there always is a prime. (4) There are infinitely many primes of the form $n^2 + 1$.

Landau, by the way, was active in the founding of the Hebrew University.

Let me state some simple solved and unsolved problems in number theory and geometry.

Prove that if $a_1 < a_2 < \ldots < a_{n+1} \leq 2n$ is any set of $n + 1$ integers not exceeding $2n$ than for some i and j $a_i \mid a_j$, i.e. you can not give $n+1$ integers $\leq 2n$ no one of which divides the other. A little more difficult is the following result which I proved in 1932 (more than 60 years ago): If $a_1 < a_2 < \ldots$ is an infinite sequence of integers no one of which divides any other, then there

[1] The Intrnational Mathematical Union, which is the organization of the mathematicians of the world, holds its international congress every four years. This year (1994) there will be such a congress in August in Zürich, Switzerland – Editor's remark.

is an absolute constant[2] c for which

$$\sum_{i=1}^{\infty} \frac{1}{a_i \log a_i} < c$$

I conjectured that[3] then in fact

$$\sum \frac{1}{a_i \log a_i} \leq \sum \frac{1}{p \log p}$$

This simple conjecture is still open and I offer 1000 shekels for a proof or disproof.

Let $a_1 < a_2 < \ldots < a_k \leq n$ be a set of integers satisfying[4] $[a_1, a_j] > n$ i.e. no integer $\leq n$ is a multiple of two a-s. I conjectured that then

$$\sum \frac{1}{a_i} \leq \frac{31}{30}$$

2,3,5, $n = 5$ shows that the conjecture is best possible. Schinzel and Szekeres proved this conjecture (Acta Scienciarum Szeged 1959). I further conjectured that for $n > n_0$ [5] $\sum \frac{1}{a_i} < 1$. In fact only two sets are known for which $\sum \frac{1}{a_i} > 1$ ($n = 5$, $a_1 = 2$, $a_2 = 3$, $a_3 = 5$ and $3, 4, 5, 7, 11$ $n = 11$). Schinzel and Szekeres proved that my conjecture, if true, is best possible. For every $\varepsilon > 0$ and $n > n_0(\varepsilon)$ they found integers $a_1 < a_2 < \ldots < a_k \leq n$, $[a_i, a_j] > n$ for which $\sum \frac{1}{a_i} > 1 - \varepsilon$. Try to find another set of integers $a_1 < a_2 < \ldots < a_k \leq n$, $[a_i, a_j] > n$, $\sum \frac{1}{a_i} > 1$. I am not at all sure if there is any such set.

There is a very simple question the solution of which can be left to the reader: Let $1 \leq a_1 < a_2 < \ldots < a_{n+2} \leq 2n$ be $n + 2$ integers not exceeding $2n$; prove that the equation $a_i + a_j = a_\ell$, $i < j < \ell$ is always solvable. The integers $n \leq t \leq 2n$ show that this simple result is best possible.

[2] Sometimes constants which appear in formulas really depend on some parameters. On the other hand, one speaks about "absolute constants" when they do not depend on anything, so they are just numbers and one could give an explicit value. One does not do so either because computing the value is difficult or because the important fact is that there is such a constant, not its numerical value – Editor's remark.

[3] p always refers to prime numbers. It is known that the series on the right-hand side converges – Editor's remark.

[4] $[a, b]$ denotes the least common multiple of a and b – Editor's remark.

[5] This expression means: there exists some n_0 such that for $n > n_0$ – Editor's remark.

More than 20 years ago in one of our papers with A. Sárközy we state the following conjecture: Let $1 \leq a_1 < a_2 < \ldots < a_{n+2} \leq 3n$ be $n+2$ integers not exceeding $3n$; prove that there always are three of them $a_i < a_j < a_k$ for which $a_i \mid (a_j + a_k)$ i.e. the smallest one divides the sum of the two larger ones. The integers $2n \leq t \leq 3n$ show that this simple conjecture, if true, is best possible. Perhaps we overlook a simple argument but we have not been able to settle this question.

Now let me state a more serious problem which attracted the attention of many great mathematicians. Schur conjectured more than 60 years ago that if we divide the integers into k classes then for every ℓ at least one of the classes contains an arithmetic progression of length[6] ℓ. Van der Waerden proved this conjecture. Denote by $f(k,\ell)$ the smallest integer for which, if we divide the integers $1 \leq t \leq f(k,\ell)$ into k classes, at least one of the classes contains an arithmetic progression of length ℓ. Van der Waerden proved that $f(k,\ell)$ exists, but he got a very large upper bound for $f(2,\ell)$, in fact his $f(2,\ell)$ increased at least as fast as the so called Ackermann function.[7] More details about this problem can be found in a book of R. L. Graham, B. Rothschild and J. Spencer entitled "Ramsey Theory" see the second edition. R. L. Graham offered 1000 dollars for the proof that

$$f(2,\ell) < 2^{2^{2^{\cdot^{\cdot^{\cdot^{2}}}}}} \qquad (\ell \text{ times}) \tag{1}$$

(1) is still open but a few years ago S. Shelah of the Hebrew University found a somewhat weaker upper bound for $f(2,\ell)$ and $f(k,\ell)$. Graham gave a consolation prize of 500 dollars to Shelah and the conjecture (1) is still open and in fact it is quite possible that

$$f(2,\ell) < 2^{c\,\ell} \tag{2}$$

for some ℓ. R Rado and I proved that $f(2,\ell) > 2^{\ell/2}$ and Berlekamp proved $f(2,\ell) > 2^{\ell}/\ell$. As far as I know it is not yet known if $f(2,\ell)/2^{\ell} \to \infty$. It would be very desirable to decide if $f(2,\ell) > (2+\varepsilon)^{\ell}$ is true.

About 60 years ago Turán and I conjectured a significant sharpening of Van der Waerden's theorem.

[6] The length of an arithmetic progression is the number of its elements. Thus $7, 11, 15$ in of length 3 – Editor's remark.

[7] About the Ackermann function, see the article by Prof. M. Sharir in "Etgar–Gilyonot Matematika" No. 29-30 – Editor's remark.

In fact we conjectured that you do not have to divide the integers into two classes to get a long arithmetic progression but every large set of integers will already contain a long arithmetic progression. More precisely: Let $r_\ell(n)$ be the smallest integer for which every set of integers $1 \leq a_1 < a_2 < \ldots < a_t \leq n$, $t = r_\ell(n)$ contains an arithmetic progression of ℓ terms. We conjectured that for every ℓ

$$r_\ell(n)/n \to 0 \tag{3}$$

Schur's conjecture (for $k = 2$) would already follow from $r_\ell(n) < \frac{n}{2}$. It is easy to see that

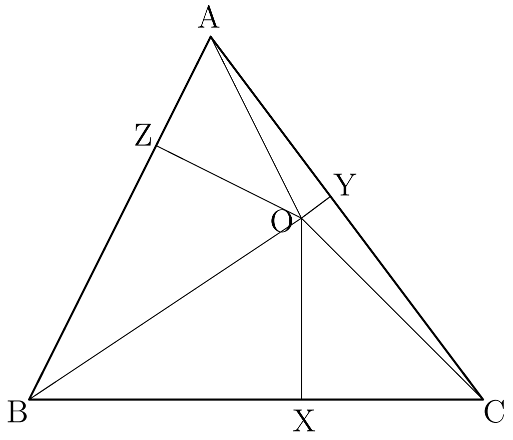
$$r_\ell(a+b) \leq r_\ell(a) + r_\ell(b) \tag{4}$$

and (4) easily implies by an old argument of Fekete that $\lim r_\ell(n)/n$ exists. The whole difficulty was to prove that the limit is 0. This was eventually accomplished by Szemerédi, Acta Arithmetica 1975 and Fürstenberg obtained a different proof (Fürstenberg is a professor at the Hebrew University). I offered a prize of 1000 dollars for a proof of (3) and Szemerédi got the well deserved prize.

There is a problem for which I offer 3000 dollars. Is it true that if $a_1 < a_2 < \ldots$ is such that $\sum \frac{1}{a_\ell} = \infty$ then the a's contain for every ℓ an arithmetic progression of length ℓ. This is open even for $\ell = 3$. The conjecture would imply that the primes contain infinitely many arithmetic progressions of length ℓ since Euler proved in 1735 that $\sum \frac{1}{p}$, p prime, diverges.[8]

Now I would like to talk about geometry. First let me state the Erdös-Mordell inequality for triangles.

[8] It is known that there are infinitely many triples of primes which form an arithmetic progression, i.e. $p + q = 2r$ is solvable for infinitely many primes, but it is not yet known if there are infinitely many quadruples of primes p_1, p_2, p_3, p_4 which form an arithmetic progression.



I conjectured this in 1932 and Mordell proved it two years later; the interested reader can find it e.g. in the book of Fejes-Toth. Let ABC be a triangle; O a point in its interior; X,Y,Z are the perpendiculars dropped from O. Prove $OA+OB+OC \geq 2(OX+OY+OZ)$; equality only if ABC is equilateral and O its center; the proof is not entirely trivial. It might be worth while to find the point O for which $\frac{OA+OB+OC}{OX+OY+OZ}$ is minimal or the point for which $OA+OB+OC-2(OX+OY+OZ)$ is minimal. I am not sure if this leads to an interesting problem.

Next Anning and I proved that if $x_1, x_2, \ldots$ is an infinite set of points in the plane and all the distances $d(x_i, x_j)$ are integers then the points are on a line. For a very simple proof see my paper in the Bull. Amer. Math. Soc. 1945.

Ulam made the following beautiful and no doubt very difficult conjecture: Let $x_1, x_2, \ldots$ be a set of points in the plane and suppose the set $x_1, \ldots$ is everywhere dense. Prove that the distances $d(x_i, x_j)$ can not all be rational. Probably a set for which all distances are rational must be very restricted. It is not yet known whether for every k there are k points in the plane in general position i.e. no three on a line and no four on a circle so that all the distances $d(x_i, x_j)$ are integers. In fact, I do not think that 7 points are known with this property.

Let there be given n points in the plane. Denote by $f(n)$ the smallest integer for which the n points determine at least $f(n)$ distinct distances. I conjectured in my paper in the Amer. Math. Monthly 1946 that

$$f(n) \geq \frac{cn}{\sqrt{\log n}} \tag{5}$$

If true (5) is best possible except for the value of c.

I offer 500 dollars for a proof or disproof of (5).

I also conjectured that if $x_1, \ldots, x_n$ forms a convex polygon then the number of distinct distances $d(x_i, x_j)$ is at least $\left[\frac{n}{2}\right]$, equality for the regular polygon. This conjecture was proved by my colleage at the Technion Altman (Amer. Math. Monthly 1963). I further conjectured that in a convex n-gon there always is a vertex x_i so that the number of distinct distances from x_i is at least $\frac{n}{2}$. This conjecture is still open.

Is it true that in a convex n-gon there is always a vertex which has no four other vertices equidistant from it?

Let $x_1, \ldots, x_n$ be n points in the plane no three on a line. Szemerédi conjectured that these points determine at least $\left[\frac{n}{2}\right]$ distinct distances. This would be a significant extension of the theorem of Altman, but the problem is still open. Szemerédi only proved that they determine at least $\frac{n}{3}$ distinct distances.

Let $x_1, \ldots, x_n$ be n points in the plane not all on a line. Sylvester (and later independently I) conjectured that there is always a line which goes through exactly two of these points. This conjecture was first proved by Gallai.[9] Join every two of the points; prove that you get at least n distinct lines.

Two more problems: E. Klein observed that among 5 points not all on a line there always are four which are the vertices of a convex quadrilateral. She asked: Let $f(n)$ be the smallest integer for which among any $f(n)$ points no three on a line there always are n of them which are the vertices of a convex n-gon. Probably $f(n) = 2^{n-2} + 1$. Szekeres and I proved

$$2^{n-2} + 1 \leq f(n) \leq \binom{2n-4}{n-2}$$

$f(5) = 9$ is known but $f(6) = 17$ is still open.

[9] The simplest proof is due to L. M. Kelly. Probably for $n > n_0$ the number of Gallai lines is $\geq \frac{n}{2}$ (i.e. the number of lines which go through exactly two of our points). This is still open. J. Csima and E. T. Sawyer proved that the number of Gallai lines is $\geq \frac{6n}{13}$.

I asked about 20 years ago: Let $x_1, \dots, x_n$ be n points in the plane; consider all the circles of radius 1 which pass through three of our points. Denote by $g(n)$ the maximum number of distinct unit circles with this property. (Circles of radius 1 are called unit circles.) I conjectured

$$\frac{g(n)}{n} \to \infty \quad , \quad \frac{g(n)}{n^2} \to 0$$

My colleage Elekes in Hungary has a very ingenious proof for $g(n) > cn^{3/2}$ (Combinatorica Vol. 4 1984). $g(n)/n^2 \to 0$ is still open.

Finally, let f(n) be the largest integer for which you can find n points $x_1, \dots, x_n$ so that every x_i, $1 \leq i \leq n$ should have $f(n)$ other x_i's equidistant from it. In particular is $f(n) > n^\varepsilon$ (ε positive) possible?