Publ. Math. Debrecen
92/1-2 (2018), 255–260
DOI: 10.5486/PMD.2018.7983

On some open problems of number theory

By ANDRZEJ SCHINZEL (Warszawa)

Abstract. I shall present here 14 open problems of number theory arranged chronologically from Antiquity to 1952, giving each time the best known partial result now and in 1952.

Antiquity has left us a definition of a perfect number and two problems concerning perfect numbers.

Definition 1. A positive integer n is *perfect* if it is the sum of its all proper divisors.

Problem 1. *Do there exist infinitely many even perfect numbers?*

Euclid's *Elements* contains a formula for even perfect numbers, which in the modern notation looks $2^{p-1}(2^p-1)$, where 2^p-1 is a prime. Euler proved that all even perfect numbers are given by this formula. Till now we know 49 even perfect numbers, the greatest being $2^{74207280}(2^{74207281}-1)$, in January 1952 we knew only 12 even perfect numbers, the greatest being $2^{126}(2^{127}-1)$ (see [5], and [2, B1]).

Problem 2. *Does there exist an odd perfect number?*

L. E. Dickson proved in 1913 that for every given k there exist only finitely many odd perfect numbers with exactly k distinct prime factors. P. Nielsen proved in 2003 that such numbers are less than 2^{4^k} (see [7, p. 15]). We now know that for odd perfect numbers n, $n > 10^{300}$, $k = \omega(n) \geq 9$, in 1952 we knew that $n > 5 \cdot 10^5$, $\omega(n) \geq 6$ (see ibid.).

Mathematics Subject Classification: 11-02.
A lecture given at the University of Debrecen on March 9, 2017, slightly enlarged and modified.

In order to reach the next open problem, we have to mention amicable numbers, studied first in the Middle Ages.

Definition 2. Positive integers $m < n$ are *amicable* if

$$s(m) = n, \quad s(n) = m,$$

where $s(n)$ is the sum of all proper divisors of n.

Antiquity had known one pair of amicable numbers 220 and 284. In the 9th century, it was shown by Thabit ben Qurra that if the numbers $p = 3 \cdot 2^n - 1$, $q = 3 \cdot 2^{n-1} - 1$, $r = 9 \cdot 2^{2n-1} - 1$ are primes for $n > 1$, then $2^n pq$ and $2^n r$ are an amicable pair. This suggests

Problem 3. *Do there exist infinitely many amicable pairs?*

We know more than 10^7 amicable pairs. The best known upper estimate for the number of amicable pairs $\langle m, n\rangle$, where $m \le x$, is

$$O\big(x \exp\big(-(1/2 + o(1))(\log x \log\log x)^{1/2}\big)\big),$$

(see [9]).

The arithmetical function $s(n)$ occurs also in Problem 10.

In order to reach next unsolved problems, we go to the 18th century. Christian Goldbach asked in a letter to Euler of 1742 the following question: *Is every integer > 2 the sum of three primes?* In Goldbach's time, differently than now, 1 had been considered a prime. Keeping this in mind we can formulate

Problem 4 (Goldbach 1742)**.** *Is every even integer $n > 2$ the sum of two primes?*

The affirmative answer has been checked for $n < 1.6 \cdot 10^{18}$ (see [7, p. 232]; in 1952, $n < 6 \cdot 10^4$). Besides, J. R. Chen showed in 1973 that all even integers large enough are sums of a prime and of a P_2 (P_k denotes the product of at most k primes). In 1952, it was known that there exists a k such that all even numbers > 2 are sums of a prime and of a P_k, see [7, p. 276]. The Goldbach problem makes sense also for odd integers. This case has been in principle solved by I. M. Vinogradov in 1937. However, the bound from which his proof worked has been huge, far exceeding the possibilities of the present day computers. Therefore, a sensation has been created by H. Helfgott, who, in 2013, diminished the bound to e^{30}, up to which the phenomenon has been checked, thus obtaining the following theorem: *every odd integer > 5 is the sum of three primes* (see [3]).

The 18th century left us another open problem, for which a definition is needed.

Definition 3. A positive integer d is "*numerus idoneus*" (a convenient number) if every odd integer representable essentially uniquely as $x^2 + dy^2$ and satisfying in this unique representation the condition $(x, dy) = 1$ is prime.

All positive integers ≤ 10 are convenient, 11 is not convenient, because $15 = 2^2 + 11 \cdot 1^2$ and $(2, 11 \cdot 1) = 1$, but 15 is not a prime.

Problem 5 (Euler 1778)**.** *Does there exist "numerus idoneus" greater than* 1848*?*

Euler found 65 convenient numbers, the greatest of which is 1848. Gauss noticed that convenient numbers d are characterized by the equation $p(-4d) = 1$, where $p(D)$ is the number of classes of positive (properly) primitive forms with discriminant D in the principal genus. S. Chowla used this characterization in his proof of 1934 that there are only finitely many convenient numbers (see [7, p. 21]). P. J. Weinberger [10] proved in 1973 that there is at most one greater than 1848 and there is none such up to $\frac{1}{4} \cdot 10^{60}$. In 1952, the relevant bound was $5 \cdot 10^4$ (see [7, p. 21]).

The outstanding problems in number theory proposed in the 19th century are well described in the lecture given by E. Landau at the International Congress of Mathematicians in 1912. They have, however, been proposed in a more general form earlier (see [7, pp. 37–39]).

Problem 6 (de Polignac 1849)**.** *Do there exist infinitely many twin primes, i.e. such pairs* (p, q) *that* p, q *are primes and* $q - p = 2$*?*

J. R. Chen proved that there exist infinitely many pairs (p, P_2), where $P_2 - p = 2$ (see [7, p. 277]). Chen has been working in China and amazing progress in Problem 6 has been made by the Chinese mathematician working in the U.S., Y. Zhang. He has proved [11] that denoting by p_n the n-th prime, we have $\liminf_{n\to\infty}(p_{n+1} - p_n) \leq 7 \cdot 10^7$. The number $7 \cdot 10^7$ has been diminished to 246, but this is unpublished. On the other hand, J. Maynard [6] proved in 2015 by a different method that $\liminf_{n\to\infty}(p_{n+1} - p_n) \leq 600$.

Problem 7 (Bouniakowsky 1857)**.** *Do there exist infinitely many primes of the form* $x^2 + 1$*?*

Bouniakowsky considered a general irreducible polynomial $f \in \mathbb{Z}[x]$ and conjectured that $\frac{f(x)}{d_f}$ represents for $x \in \mathbb{N}$ infinitely many primes (positive or negative), where d_f is the fixed divisor of f (see [1, p. 333]).

Let us put $d = \deg f$ and assume that f has the leading coefficient positive. If $d = 1$, Bouniakowsky's conjecture becomes Dirichlet's theorem on arithmetic

progression. In general, A. Buchstab in 1967 and H.-E. Richert in 1969 proved that $\frac{f(x)}{d_f}$ represents for $x \in \mathbb{N}$ infinitely many P_{d+1}, and for $d = 2$, H. Iwaniec proved in 1998 that P_3 can be replaced by P_2, see [7, p. 76]. J. Friedlander and H. Iwaniec proved in 1998 that $x^2 + y^4$ represents infinitely many primes, see [7, p. 324].

In order to formulate Riemann's problem, probably the most important problem of mathematics, in an elementary form, we need a definition.

Definition 4. $\pi(x)$ is the number of primes $\leq x$,

$$\operatorname{li} x = \int_0^x \frac{dt}{\log t} = C + \int_2^x \frac{dt}{\log t}.$$

Problem 8 (Riemann 1859 – von Koch 1901)**.** *Does there exist a constant A such that for every positive x*

$$|\pi(x) - \operatorname{li} x| < A\sqrt{x}\,\log x?$$

The affirmative answer to this problem is equivalent to the Riemann Hypothesis (see [7, p. 31]). We even do not know for any positive $\varepsilon < \frac{1}{2}$ the inequality

$$|\pi(x) - \operatorname{li} x| < A_\varepsilon x^{1-\varepsilon},$$

and the best known result in this direction proved by Korobov and Vinogradov in 1958 is

$$|\pi(x) - \operatorname{li} x| < Axe^{-c(\log x)^{3/5}(\log\log x)^{-1/5}},$$

where c is a positive constant.

In 1952, the exponent of $\log x$ had been any number less than $\frac{4}{7}$ (see [7, p. 199–200]).

Problem 9 (Oppermann 1882)**.** *Does there exist a prime between every pair of consecutive squares?*

The problem concerns $d_n = p_{n+1} - p_n$, as does Problem 6, and asks roughly whether

$$d_n < 2\sqrt{p_n}. \qquad (*)$$

The last known estimate valid for all n is $d_n < Ap_n^{0.525}$ due to R. Baker, G. Harman and J. Pintz, in 1952 the last available estimate was $d_n < Ap_n^{48/77}$ (see [7, pp. 141–142]). H. Cramér proved in 1921 that assuming the affirmative answer to Problem 8, the density of indices n such that $(*)$ holds is one (see [7, p. 140]).

Problem 10 (Catalan 1887 – Dickson 1913)**.** *If $s(0) = 0$, is the sequence $n, s(n), ss(n), \ldots$ bounded for every positive integer n?*

For perfect n the sequence has period of length 1, for amicable n and $s(n)$, of length 2. For an inconclusive evidence that the answer to this problem may be negative, see [2, B6].

Passing to the 20th century, we again need a definition.

Definition 5. $\varphi(n)$ is the number of positive integers $\leq n$ and prime to n.

Problem 11 (Carmichael 1907–1922)**.** *Does there exist an integer m such that the equation $\varphi(x) = m$ has exactly one solution?*

R. Carmichael in 1907 had an alleged proof of the negative answer, in 1922, he found an error in the proof and asked the problem. In 1952, it was known that $m > 10^{400}$, now it is known that $m > 10^{10^{10}}$, see [7, p. 21] and [2, B39].

Problem 12 (Pillai 1945)**.** *Does the difference between consecutive perfect powers tend to infinity?*

The affirmative answer to the problem is equivalent to finiteness of solutions of the Diophantine equation $x^z - y^t = d$, $z, t \geq 1$, for every positive integer d. R. Tijdeman proved in 1976 the finiteness for $d = 1$, and P. Mihailescu proved in 2004 that 8 and 9 form the only pair of consecutive perfect powers differing by 1.

The next two problems are partially due to the famous Hungarian mathematician, P. Erdős.

Problem 13 (Erdős and Straus 1948)**.** *Has the equation*

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

a solution in positive integers for all $n > 1$?

The affirmative answer is known for $n < 10^{14}$ (see [7, p. 312] and [2, D11]), in 1952 it had been proved for $n \leq 106128$, see [8].

To formulate Problem 14, we need a definition.

Definition 6. A system of congruences $x \equiv a_i \pmod{m_i}$ $(1 \leq i \leq k)$ is *covering* if every integer x satisfies at least one of the congruences.

Problem 14 (Erdős and Selfridge 1952)**.** *Does there exist a covering system with distinct odd moduli $m_i > 1$?*

For a long time, Erdős proposed a problem, whether there exists a covering system with distinct moduli m_i arbitrarily large. This has been answered negatively by B. Hough [4]. He proved in 2015 that in every covering system with distinct moduli $\min_{1\le i\le k} m_i \le 10^{16}$.

References

[1] L. E. Dickson, History of the Theory of Numbers, Vol. I., Reprint, *Chelsea Publishing Co.*, *New York*, 1952.

[2] R. K. Guy, Unsolved Problems in Number Theory, 3rd edition, *Springer-Verlag*, *New York*, 2004.

[3] H. A. Helfgott, La conjecture de Goldbach ternaire, *Gaz. Math.* **140** (2014), 5–18.

[4] B. Hough, Solution of the minimum modulus problem for covering systems, *Ann. of Math. (2)* **181** (2015), 361–382.

[5] https://primes.utm.edu/mersenne/

[6] J. Maynard, Small gaps between primes, *Ann. of Math. (2)* **181** (2015), 383–413.

[7] W. Narkiewicz, Rational Number Theory in the 20th Century. From PNT to FLT, *Springer*, *London*, 2012.

[8] R. Obláth, Sur l'équation diophantienne $\frac{4}{n} = \frac{1}{x} + \frac{1}{y} + \frac{1}{z}$, *Mathesis* **59** (1950), 308–316.

[9] C. Pomerance, On amicable numbers, In: Analytic Number Theory, *Springer*, *Cham*, 2015, 321–327.

[10] P. J. Weinberger, Exponents of the class groups of complex quadratic fields, *Acta Arith.* **22** (1973), 117–124.

[11] Y. Zhang, Bounded gaps between primes, *Ann. of Math. (2)* **179** (2014), 1121–1174.

ANDRZEJ SCHINZEL
INSTITUTE OF MATHEMATICS OF THE
POLISH ACADEMY OF SCIENCES
ŚNIADECKICH 8
00-656 WARSZAWA
POLAND

E-mail: schinzel@impan.pl

(Received March 24, 2017)