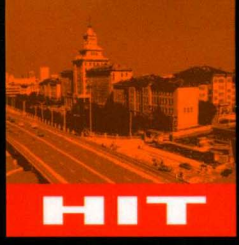
Problem-Solving and Selected Topics in Number Theory in the Spirit of the Mathematical Olympiads



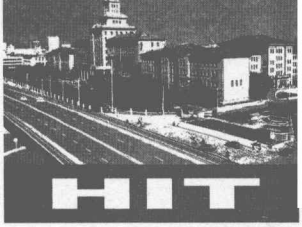
国外优秀数学著作
原 版 系 列

用数学奥林匹克精神解数论问题

[希] 迈克尔·罗西亚斯 (Michael Th. Rassias) 著

哈尔滨工业大学出版社
HARBIN INSTITUTE OF TECHNOLOGY PRESS

用数学奥林匹克精神解数论问题



国外优秀数学著作
原版系列

用数学奥林匹克精神解数论问题

Problem-Solving and Selected Topics in Number Theory in the Spirit of the Mathematical Olympiads

[希]迈克尔·罗西亚斯（Michael Th. Rassias）著

哈尔滨工业大学出版社
HARBIN INSTITUTE OF TECHNOLOGY PRESS

黑版贸审字 08-2017-046 号

图书在版编目(CIP)数据

用数学奥林匹克精神解数论问题 = Problem-Solving and Selected Topics in Number Theory in the Spirit of the Mathematical Olympiads:英文/(希)迈克尔·罗西亚斯(Michael Th. Rassias)著. —哈尔滨:哈尔滨工业大学出版社,2018.1
ISBN 978-7-5603-6913-6

Ⅰ.①用… Ⅱ.①迈… Ⅲ.①数论-研究-英文
Ⅳ.①O156

中国版本图书馆 CIP 数据核字(2017)第 218862 号

策划编辑 刘培杰
责任编辑 张永芹 钱辰琛
封面设计 孙茵艾
出版发行 哈尔滨工业大学出版社
社 址 哈尔滨市南岗区复华四道街 10 号 邮编 150006
传 真 0451-86414749
网 址 http://hitpress.hit.edu.cn
印 刷 哈尔滨市工大节能印刷厂
开 本 787mm×1092mm 1/16 印张 23.25 字数 498 千字
版 次 2018 年 1 月第 1 版 2018 年 1 月第 1 次印刷
书 号 ISBN 978-7-5603-6913-6
定 价 108.00 元

To my father Themistocles

Foreword

The International Mathematics Olympiad (IMO), in the last two decades, has become an international institution with an impact in most countries throughout the world, fostering young mathematical talent and promoting a certain approach to complex, yet basic, mathematics. It lays the ground for an open, unspecialized understanding of the field to those dedicated to this ancient art.

The tradition of mathematical competitions is sometimes traced back to national contests which were organized in some countries of central Europe already at the beginning of the last century. It is very likely that a slight variation of the understanding of mathematical competition would reveal even more remote ancestors of the present IMO. It is, however, a fact that the present tradition was born after World War II in a divided Europe when the first IMO took place in Bucharest in 1959 among the countries of the Eastern Block. As an urban legend would have it, it came about when a high school mathematics teacher from a small Romanian town began to pursue his vision for an organized event that would help improve the teaching of mathematics.

Since the early beginnings, mathematical competitions of the international olympiad type have established their own style of problems, which do not require wide mathematical background and are easy to state. These problems are nevertheless difficult to solve and require imagination plus a high degree of original thinking. The Olympiads have reached full maturity and worldwide status in the last two decades. There are presently over 100 participating countries.

Accordingly, quite a few collections of Olympiad problems have been published by various major publishing houses. These collections include problems from past olympic competitions or from among problems proposed by various participating countries. Through their variety and required detail of solution, the problems offer valuable training for young students and a captivating source of challenges for the mathematically interested adult.

In the so-called Hall of Fame of the IMO, which includes numerous presently famous mathematicians and several Fields medalists, one finds a

list of the participants and results of former mathematical olympiads (see [HF]). We find in the list of the participants for Greece, in the year 2003, the name of Michael Th. Rassias. At the age of 15 at that time, he won a silver medal and achieved the highest score on the Greek team. He was the first Greek of such a young age in over a decade, to receive a silver medal. He is the author of the present book: one more book of Olympiad Problems among other similar beautiful books.

Every single collection adds its own accent and focus. The one at hand has a few particular characteristics which make it unique among similar problem books. While most of these books have been written by experienced mathematicians after several decades of practicing their skills as a profession, Michael wrote this present book during his undergraduate years in the Department of Electrical and Computer Engineering of the National Technical University of Athens. It is composed of some number theory fundamentals and also includes some problems that he undertook while training for the olympiads. He focused on problems of number theory, which was the field of mathematics that began to capture his passion. It appears like a confession of a young mathematician to students of his age, revealing to them some of his preferred topics in number theory based on solutions of some particular problems—most of which also appear in this collection. Michael does not limit himself to just those particular problems. He also deals with topics in classical number theory and provides extensive proofs of the results, which read like "all the details a beginner would have liked to find in a book" but are often omitted.

In this spirit, the book treats Legendre symbols and quadratic reciprocity, the Bertrand Postulate, the Riemann ζ-function, the Prime Number Theorem, arithmetic functions, diophantine equations, and more. It offers pleasant reading for young people who are interested in mathematics. They will be guided to an easy comprehension of some of the jewels of number theory. The problems will offer them the possibility to sharpen their skills and to apply the theory.

After an introduction of the principles, including Euclid's proof of the infinity of the set of prime numbers, follows a presentation of the extended Euclidean algorithm in a simple matricial form known as the Blankinship method. Unique factorization in the integers is presented in full detail, giving thus the basics necessary for the proof of the same fact in principal ideal domains. The next chapter deals with rational and irrational numbers and supplies elegant comprehensive proofs of the irrationality of e and π, which are a first taste of Rassias's way of breaking down proofs in explicit, extended steps.

The chapter on arithmetic functions presents, along with the definition of the Möbius μ and Euler ϕ functions, the various sums of divisors

$$\sigma_a(n) = \sum_{d|n} d^a,$$

as well as nice proofs and applications that involve the Möbius inversion formula. We find a historical note on Möbius, which is the first of a sequence of such notes by which the author adds a temporal and historical frame to the mathematical material.

The third chapter is devoted to algebraic aspects, perfect numbers, Mersenne and Fermat numbers, and an introduction to some open questions related to these. The fourth deals with congruences, the Chinese Remainder Theorem, and some results on the rings $\mathbb{Z}/(n \cdot \mathbb{Z})$ in terms of congruences. These results open the door to a large number of problems contained in the second part of the book.

Chapter 5 treats the symbols of Legendre and Jacobi and gives Gauss's first geometric proof of the law of quadratic reciprocity. The algorithm of Solovay and Strassen—which was the seminal work leading to a probabilistic perspective of fundamental notions of number theory, such as primality—is described as an application of the Jacobi symbol. The next chapters are analytic, introducing the ζ and Dirichlet series. They lead to a proof of the Prime Number Theorem, which is completed in the ninth chapter. The tenth and eleventh chapters are, in fact, not only a smooth transition to the problem part of the book, containing already numerous examples of solved problems, they also, at the same time, lead up to some theorems. In the last two subsections of the appendix, Michael discusses special cases of Fermat's Last Theorem and Catalan's conjecture.

I could close this introduction with the presentation of *my favorite problem*, but instead I shall present and briefly discuss another short problem which is included in the present book. It is a *conjecture* that Michael Rassias conceived of at the age of 14 and tested intensively on the computer before realizing its intimate connection with other deep conjectures of analytic number theory. These conjectures are still today considered as intractable.

Rassias Conjecture. For any prime p with $p > 2$ there are two primes p_1, p_2, with $p_1 < p_2$ such that

$$p = \frac{p_1 + p_2 + 1}{p_1}. \tag{1}$$

The conjecture was verified empirically on a computer and was published along with a series of problems from international Olympiads (see [A]). The purpose of this short note is to put this conjecture in its mathematical context and relate it to further known conjectures.

At first glance, the expression (1) is utterly surprising and it could stand for some unknown category of problems concerning representation of primes. Let us, though, develop the fraction in (1):

$$(p-1)p_1 = p_2 + 1.$$

Since p is an odd prime, we obtain the following slightly more general conjecture: *For all $a \in \mathbb{N}$ there are two primes p, q such that*

$$2ap = q + 1. \tag{2}$$

Of course, if (2) admits a solution for any $a \in \mathbb{N}$, then a fortiori (1) admits a solution. Thus, the Rassias conjecture is true. The new question has the particularity that it only asks to prove the existence of a single solution. We note, however, that this question is related to some famous problems, in which one asks more generally to show that there is an infinity of primes verifying certain conditions.

For instance, the question if there is an infinity of Sophie Germain primes p, i.e., primes such that $2p + 1$ is also a prime, has a similar structure. While in the version (2) of the Rassias conjecture, we have a free parameter a and search for a pair (p, q), in the Sophie Germain problem we may consider p itself as a parameter subject to the constraint that $2p + 1$ is prime, too. The fact that there is an infinity of Sophie Germain primes is an accepted conjecture, and one expects the density of such primes to be $O(x/\ln^2(x))$ [Du]. We obtain from this the modified Rassias conjecture by introducing a constant a as factor of 2 and replacing $+1$ by -1. Thus $q = 2p + 1$ becomes $q = 2ap - 1$, which is (2). Since a is a parameter, in this case we do not know whether there are single solutions for each a. When a is fixed, this may of course be verified on a computer or symbolically.

A further related problem is the one of Cunningham chains. Given two coprime integers m, n, a Cunningham chain is a sequence $p_1, p_2, \ldots, p_k$ of primes such that $p_{i+1} = mp_i + n$ for $i > 1$. There are competitions for finding the longest Cunningham chains, but we find no relevant conjectures related to either length or frequencies of such chains. In relation to (2), one would rather consider the Cunningham chains of fixed length 2 with $m = 2a$ and $n = -1$. So the question (2) reduces to the statement: *there are Cunningham chains of length two with parameters* $2a, -1$, *for any* $a \in \mathbb{N}$.

By usual heuristic arguments, one should expect that (2) has an infinity of solutions for every fixed a. The solutions are determined by one of p or q via (2). Therefore, we may define

$$S_x = \{p < ax \ : \ p \text{ is prime and verifies (2)}\}$$

and the counting function $\pi_r(x) = |S_x|$. There are $O(\ln(x))$ primes $p < x$, and $2ap - 1$ is an odd integer belonging to the class -1 modulo $2a$. Assuming that the primes are equidistributed in the residue classes modulo $2a$, we obtain the expected estimate:

$$\pi_r(x) \sim x/\ln^2(x) \tag{3}$$

for the density of solutions to the extended conjecture (2) of Rassias.

Probably the most general conjecture on distribution of prime constellations is Schinzel's *Conjecture H*:

Conjecture H. Consider s polynomials $f_i(x) \in \mathbb{Z}[X], i = 1, 2, \ldots, s$ with positive leading coefficients and such that the product $F(X) = \prod_{i=1}^{s} f_i(x)$ is not

divisible, as a polynomial, by any integer different from ± 1. Then there is at least one integer x for which all the polynomials $f_i(x)$ take prime values.

Of course, the Rassias conjecture follows for $s = 2$ with $f_1(x) = x$ and $f_2(x) = 2ax - 1$. Let us finally consider the initial problem. Can one prove that (2) has at least one solution in primes p, q, for arbitrary a? In [SW], Schinzel and Sierpiński show that Conjecture H can be stated for one value of x or for infinitely many values of x, since the two statements are equivalent. Therefore, solving the conjecture of Rassias is as difficult as showing that there are infinitely many prime pairs verifying (2). Of course, this does not exclude the possibility that the conjecture could be proved easier for certain particular families of values of the parameter a.

The book is self-contained and rigorously presented. Various aspects of it should be of interest to graduate and undergraduate students in number theory, high school students and the teachers who train them for the Putnam Mathematics Competition and Mathematical Olympiads as well as, naturally, to scholars who enjoy learning more about number theory.

Bibliography

[A] T Andreescu and D. Andrica, *Number Theory*, Birkhäuser, Boston, (2009), p. 12.

[Du] H Dubner, *Large Sophie-Germain primes*, Math. Comp., 65(1996), pp. 393–396.

[HF] *http://www.imo-official.org/country_hall.aspx?code=HEL*

[R] Michael Th. Rassias, *Open Problem No. 1825*, Octogon Mathematical Magazine, 13(2005), p. 885. See also Problem 25, Newsletter of the European Mathematical Society, 65(2007), p. 47.

[SW] A Schinzel and W. Sierpiński, *Sur certaines hypothèses concernant les nombres premiers*, Acta Arith., 4(1958), pp. 185–208.

Preda Mihăilescu
Mathematics Institute
University of Göttingen
Germany

Acknowledgments

I wish to express my gratitude to Professors A. Papaioannou and V. Papanicolaou for their invaluable assistance and inspirational guidance, both during my studies at the National Technical University of Athens and the preparation of this book.

I feel deeply honored that I had the opportunity to communicate with Professor Preda Mihăilescu, who has been my mentor in Mathematics since my high school years and has written the Foreword of the book.

I would like to thank Professors M. Filaseta, S. Konyagin, V. Papanicolaou and J. Sarantopoulos for their very helpful comments concerning the step-by-step analysis of Newman's proof of the Prime Number Theorem. Professor P. Pardalos has my special appreciation for his valuable advice and encouragement. I would like to offer my sincere thanks to Professors K. Drakakis, J. Kioustelidis, V. Protassov and J. Sandor for reading the manuscript and providing valuable suggestions and comments which have helped to improve the presentation of the book.

This book is essentially based on my undergraduate thesis on computational number theory, which I wrote under the supervision of Professors A. Papaioannou, V. Papanicolaou and C. Papaodysseus at the National Technical University of Athens. I have added a large number of problems with their solutions and some supplementary number theory on special topics.

I would like to express my thanks to my teachers for their generous advice and encouragement during my training for the Mathematical Olympiads and throughout my studies.

Finally, it is my pleasure to acknowledge the superb assistance provided by the staff of Springer for the publication of the book.

Michael Th. Rassias

Contents

1

Introduction

God created the natural numbers. The rest is the work of man.
Leopold Kronecker (1823–1891)

Number Theory is one of the most ancient and active branches of pure mathematics. It is mainly concerned with the properties of integers and rational numbers. In recent decades, number theoretic methods are also being used in several areas of applied mathematics, such as cryptography and coding theory.

In this section, we shall present some basic definitions, such as the definition of a prime number, composite number, rational number, etc. In addition, we shall present some basic theorems.

1.1 Basic notions

Definition 1.1.1. *An integer p greater than* 1 *is called a* ***prime number****, if and only if it has no positive divisors other than* 1 *and itself.*

Hence, for example, the integers 2, 3, 13, 17 are *prime numbers*, but 4, 8, 12, 15, 18, 21 are not.

The natural number 1 is not considered to be a prime number.

Definition 1.1.2. *All integers greater than one which are not prime numbers are called* ***composite numbers****.*

Definition 1.1.3. *Two integers a and b are called* ***relatively prime*** *or* ***coprime*** *if and only if there does not exist another integer c greater than* 1*, which can divide both a and b.*

For example, the integers 12 and 17 are *relatively prime.*

M.Th. Rassias, *Problem-Solving and Selected Topics in Number Theory: In the Spirit of the Mathematical Olympiads*, DOI 10.1007/978-1-4419-0495-9_1,

Prime numbers are, in a sense, the building blocks with which one can construct all integers. At the end of this chapter we are going to prove the *Fundamental Theorem of Arithmetic* according to which every natural number greater than one can be represented as the product of powers of prime numbers in a unique way.

This theorem was used by the ancient Greek mathematician Euclid, in order to prove that prime numbers are infinitely many.

We shall now present the proof of the fact that the number of primes is infinite. The following proof is due to Euclid and is considered to be one of the most elementary and elegant proofs of this theorem.

Lemma 1.1.4. *The least nontrivial divisor of every positive integer greater than 1 is a prime number.*

Proof. Let $n \in \mathbb{N}$, with $n > 1$ and d_0 be the least nontrivial divisor of n. Let us also suppose that d_0 is a composite positive integer. Then, since d_0 is composite, it must have a divisor m, with $1 < m < d_0$. But, in that case, m would also divide n and therefore d_0 would not be the least nontrivial divisor of n. That contradicts our hypothesis and hence completes the proof of the lemma. □

Theorem 1.1.5 (Euclid). *The number of primes is infinite.*

Proof. Let us suppose that the number of primes is finite and let p be the greatest prime number. We consider the integer

$$Q = p! + 1.$$

Therefore, if Q is a prime number it must be greater than p. But, this contradicts the property of p being the greatest prime number. On the other hand, if Q is not a prime number, then by the previous lemma it follows that it will certainly have prime divisors. However, if Q is divided by any prime number less than or equal to p, it leaves remainder 1. Thus, every prime divisor of Q is necessarily greater than p, which again contradicts the property of p.

So, the hypothesis that the number of primes is finite, leads to a contradiction. Hence, the number of primes is infinite. □

We shall now proceed to the proof of a theorem which is known as **Bezout's Lemma** or the **extended Euclidean algorithm**.

Theorem 1.1.6. *Let $a, b \in \mathbb{Z}$, where at least one of these integers is different than zero. If d is the greatest positive integer with the property $d \mid a$ and $d \mid b$, then there exist $x, y \in \mathbb{Z}$ such that $d = ax + by$.*

Proof. Let us consider the nonempty set

$$A = \{ax + by \mid a, b, x, y \in \mathbb{Z}, \text{ with } ax + by > 0\}.$$

We shall prove that the integer d is the least element in A.

Let d' be the least element in A. Then, there exist integers q, r, such that

$$a = d'q + r,\ 0 \leq r < d.$$

We are going to prove that $d' \mid a$. In other words, we will show that $r = 0$.

Let $r \neq 0$, then

$$r = a - d'q = a - (ax_1 + by_1)q,$$

for some integers x_1, y_1.

Therefore,

$$r = a(1 - x_1q) + b(-y_1q).$$

But, by the assumption we know that $r \neq 0$. Hence, it is evident that $r > 0$ and $r = ax_2 + by_2$, with $x_2 = 1 - x_1$, $y_2 = -y_1q \in \mathbb{Z}$. However, this is impossible due to the assumption that d' is the least element in A. Thus, $r = 0$, which means that $d' \mid a$. Similarly, we can prove that $d' \mid b$.

So, d' is a common divisor of a and b. We shall now prove that d' is the greatest positive integer with that property.

Let m be a common divisor of a and b. Then $m|ax + ay$ and thus $m \mid d'$, from which it follows that $m \leq d'$. Consequently, we obtain that

$$d' = d = ax + by, \text{ for } x, y \in \mathbb{Z}. \qquad \square$$

Remark 1.1.7. The positive integer d with the property stated in the above theorem is unique. This happens because if there were two positive integers with that property, then it should hold $d_1 \leq d_2$ and $d_2 \leq d_1$. Thus, $d_1 = d_2$.

As a consequence of the above theorem we obtain the following corollary.

Corollary 1.1.8. *For every integer e with $e \mid a$ and $e \mid b$, it follows that $e \mid d$.*

Definition 1.1.9. *Let $a, b \in \mathbb{Z}$, where at least one of these integers is nonzero. An integer $d > 0$ is called the* ***greatest common divisor of a and b*** *(and we write d=gcd(a, b)) if and only if $d \mid a$ and $d \mid b$ and for every other positive integer e for which $e \mid a$ and $e \mid b$ it follows that $e \mid d$.*[1]

Theorem 1.1.10. *Let $d = \gcd(a_1, a_2, \ldots, a_n)$, where $a_1, a_2, \ldots, a_n \in \mathbb{Z}$. Then*

$$\gcd\left(\frac{a_1}{d}, \frac{a_2}{d}, \ldots, \frac{a_n}{d}\right) = 1.$$

Proof. It is evident that $d \mid a_1, d \mid a_2, \ldots, d \mid a_n$. Hence,

$$a_1 = k_1d, a_2 = k_2d, \ldots, a_n = k_nd, \tag{1}$$

[1] Similarly one can define the greatest common divisor of n integers, where at least one of them is different than zero.

where $k_i \in \mathbb{Z}$ for $i = 1, 2, \ldots, n$. Let

$$\left(\frac{a_1}{d}, \frac{a_2}{d}, \ldots, \frac{a_n}{d}\right) = d' > 1.$$

Then, similarly we obtain

$$d' \mid \frac{a_1}{d}, d' \mid \frac{a_2}{d}, \ldots, d' \mid \frac{a_n}{d}.$$

Consequently, there exist integers $k_1', k_2', \ldots, k_n'$, for which

$$\frac{a_1}{d} = k_1' d', \frac{a_2}{d} = k_2' d', \ldots, \frac{a_n}{d} = k_n' d'. \tag{2}$$

Therefore, by (1) and (2) we get

$$a_1 = k_1' d' d, a_2 = k_2' d' d, \ldots, a_n = k_n' d' d.$$

Thus,

$$d'd \mid a_1, d'd \mid a_2, \ldots, d'd \mid a_n.$$

Hence, $dd' \mid d$, which is impossible since $d' > 1$. Therefore, $d' = 1$. □

Theorem 1.1.11. *Let $a, b, c \in \mathbb{Z}$ and $a \mid bc$. If $\gcd(a, b) = 1$, then $a \mid c$.*

Proof. If $\gcd(a, b) = 1$, then

$$1 = ax + by, \text{ where } x, y \in \mathbb{Z}.$$

Therefore,

$$c = acx + bcy.$$

But, since $a \mid acx$ and $a \mid bcy$, it yields $a \mid c$. □

1.2 Basic methods to compute the greatest common divisor

Let $a, b \in \mathbb{Z}$. One way to compute the greatest common divisor of a and b is to find the least element in the set

$$A = \{ax + by \mid a, b, x, y \in \mathbb{Z}, \text{ with } ax + by > 0\}.$$

However, there is a much more effective method to compute $\gcd(a, b)$ and is known as the *Euclidean algorithm*.