NUMBER THEORY AND APPLICATIONS

Katsuya MIYAKE
The Graduate School of Science and Engineering, Waseda University, Japan

Keywords: well-ordered structure, mathematical induction, figure numbers, prime numbers, fundamental theorem of arithmetic, Euclidean algorithm, Pell's Equations, Pythagorean triples, Chinese remainder theorem, quadratic reciprocity law, Caesar's cipher, discrete logarithm problem, public key cryptology, prime number theorem, Riemann hypothesis, cyclotomic fields, Kronecker-Weber theorem, Kronecker's dream in his youth, complex multiplication, class field theory

Contents

Summary

Number theory is one of the oldest disciplines, and has been provided various important mathematical concepts and structures. After introducing the basic structures in natural numbers, fundamental concepts and findings such as Euclidean algorithm, prime numbers, the fundamental theorem of arithmetic, and congruence relations are explained. Then conceptual structures of cryptology are introduced as an application. Some analytic methods in number theory are good examples to see how influential the discipline is to other branches of mathematics and vice versa. Arithmetic of quadratic fields and cyclotomic fields supply clear views over a part of new harmonious lands of algebra.

1. The Additive Structure of Natural Numbers

1.1. The Well-Ordered Structure and the Principle of Mathematical Induction

The natural numbers are generated by 1 and the operation ‘$+1$’ under its additive structure: $1, 2 := 1+1, 3 := (1+1)+1 = 2+1, \ldots$ The addition in the set of natural numbers $\mathbb{N}$ is commutative and associative: $a+b = b+a, (a+b)+c = a+(b+c)$ for $a, b, c \in \mathbb{N}$.

The Well-Ordered Structure. The set $\mathbb{N}$ is *well-ordered*; that is, every non-empty subset of it has the minimum element.
The well-ordered structure of $\mathbb{N}$ implies a powerful logical method, *mathematical induction*.

The Principle of Mathematical Induction. Suppose that a finite or infinite number of propositions are parameterized by natural numbers: $P_n, n = 1, 2, 3, \ldots$ Suppose further that (i) P_1 is true, and (ii) there exists a proof of the statement that P_n implies P_{n+1} for every n. Then all propositions $P_n, n = 1, 2, 3, \ldots$, are true.

Indeed, assume that there might be a false proposition P_m. Then the subset

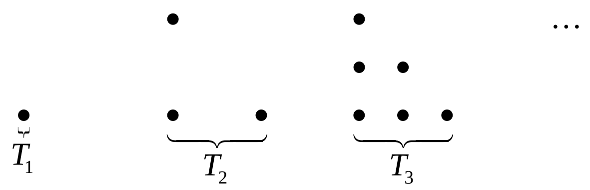
$$S := \{m \mid m \in \mathbb{N}, \text{and } P_m \text{ is false.}\}$$

of $\mathbb{N}$ is not empty. Hence there is the minimum m_0 of S. The presupposition (i) implies $m_0 > 1$. Put $n := m_0 - 1$. By the choice of m_0, P_n is true. Therefore by the presupposition (ii), $P_{n+1} = P_{m_0}$ is also true. This contradicts the choice of m_0 from S.

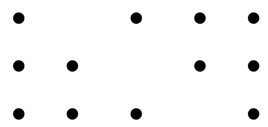
Examples are in the following subsection.

1.2.. Triangular Numbers and Square Numbers

The traditional and simplest *figure numbers* are *triangular numbers* $T_n = n(n+1)/2, n = 1, 2, 3, \ldots$, classically defined by the series of figures



Hence $T_1 = 1, T_2 = 1 + 2 = 3, \ldots, T_{n+1} = T_n + (n+1), \ldots,$ for $n \geq 1$. On one hand, we have $T_n = 1 + 2 + \cdots + n$ for $n \geq 1$. On the other hand, the figure

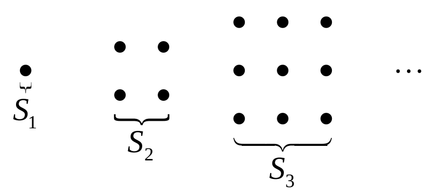


gives $2T_n = T_n + T_n = n(n+1)$. Hence we have the proposition,

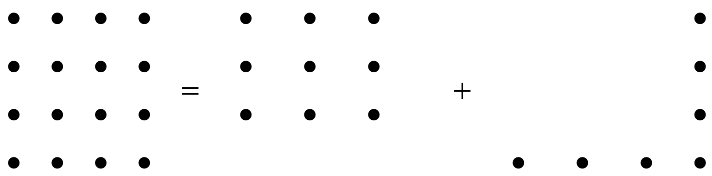
$$P_n : 1 + 2 + \cdots + n = \frac{n(n+1)}{2}. \tag{1}$$

It is clear that (i) P_1 is true. Since $n(n+1)/2 + (n+1) = (n+1)(n+2)/2$, (ii) there is a proof of the statement that P_n implies P_{n+1}. Therefore the formula of P_n is true for every $n \in \mathbb{N}$.

Square numbers $S_n = n^2, n = 1, 2, 3, \ldots,$ are defined by the series of figures



Hence $S_1 = 1, S_2 = 2^2 = 4, \ldots, S_n = n^2, \ldots,$ for $n \geq 1$. The figure



shows $S_{n+1} = S_n + (2n+1)$; that is, $(n+1)^2 = n^2 + 2n + 1$ for $n \geq 1$. We also see that

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

Mathematical induction provides the formula on the sum of odd numbers,

$$1 + 3 + \cdots + (2n+1) = (n+1)^2. \qquad (2)$$

Ancient Greeks expressed the Eqs. (1) and (2) by the above figures.

2. The Multiplicative Structure of Natural Numbers

2.1. Prime Numbers

The multiplication of natural numbers is commutative and associative:

$$a \cdot b = b \cdot a, (a \cdot b) \cdot c = a \cdot (b \cdot c), a, b, c \in \mathbb{N}.$$

To obtain a set of generators of whole natural numbers under multiplication, we need 2, then $3, 5, 7$, and so on, and all prime numbers. A *prime number* is a natural number other than 1 which cannot be expressed as a product of smaller numbers. In other words, it is only divisible by 1 and itself.

The Fundamental Theorem of Arithmetic. All prime numbers form an independent generator system of $\mathbb{N}$ under multiplication. Namely, each natural number n other than 1 is uniquely expressed as a product of a finite number of powers of primes: $n = p_1^{e_1} p_2^{e_2} \cdots p_m^{e_m}$ where $p_1, \ldots, p_m$ are distinct prime numbers and $e_1, \ldots, e_m$ are natural numbers.

There exist infinitely many prime numbers as we see in the next subsection. If we notice, therefore, the exponents $e_1, \ldots, e_m$ in the product expression, we see infinitely many copies of $\mathbb{N}$ with addition inside one $\mathbb{N}$ with multiplication.

2.2. Infinitude of Prime Numbers and Euler Product

Euclid's proof of infinitude of prime numbers in his *Elements* may be modernized as follows: let $p_1, p_2, \ldots, p_m$ be prime numbers different among themselves, and put $N := p_1 p_2 \cdots p_m + 1$; then each prime divisor p of N is different from anyone of $p_1, p_2, \ldots, p_m$. This shows that the number of prime numbers can not be finite.

L. Euler (1707–83) developed analytic methods. Let $s>1$ be a real number. Then the formula

$$1+\frac{1}{2^s}+\frac{1}{3^s}+\cdots+\frac{1}{n^s}+\cdots=\prod_p\left(1-\frac{1}{p^s}\right)^{-1} \tag{3}$$

holds; here the last product is taken over all prime numbers, and called an *Euler product*. This equality follows from the Fundamental Theorem of Arithmetic by inserting

$$\left(1-\frac{1}{p^s}\right)^{-1}=1+\frac{1}{p^s}+\frac{1}{p^{2s}}+\cdots+\frac{1}{p^{ns}}+\cdots$$

into the right hand side of (3). If the total number of primes were finite, then the right hand side of (3) would have a definite value when s tends to 1. The left hand side, however, grows to infinity when s tends to 1 because the *harmonic series* diverges to infinity. This shows the infinitude of prime numbers.

2.3. Euclidean Algorithm and the Greatest Common Divisors

Let m and n be two natural numbers, and suppose $n>m$. By subtracting m from n as many times as possible, we have

$$n=q\cdot m+r,\qquad 0\le r<m.$$

The number r thus determined is called the *residue of* n *modulo* m. If the residue is equal to 0, we say that m *divides* n, and write it as $m|n$; we also say that m is a *divisor* or a *factor* of n, and that n is a *multiple* of m.

Put $m_1:=n, m_2:=m$, and determine a series of numbers $m_1>m_2>\cdots>m_j>m_{j+1}=0$ by

$$m_i=q^{(i)}m_{i+1}+m_{i+2},\qquad 0\le m_{i+2}<m_{i+1},\quad i=1,2,\ldots,j-1. \tag{4}$$

Then $d:=m_j$ is the *greatest common divisor* of m and n, and denoted by $d=\gcd(m,n)$ or simply $d=(m,n)$ in the context of number theory.

The process (4) is called *Euclidean Algorithm* to obtain the greatest common divisor of two natural numbers. By converting the equalities of (4) into $m_{i+2}=m_i-q^{(i)}m_{i+1}, i=j-2,\ldots,1$, we obtain the following proposition:

The Greatest Common Divisor. Let m and n be two natural numbers. Then there exist two integers a and b which satisfy the equation

$$\gcd(m,n) = a \cdot m + b \cdot n, \qquad a,b \in \mathbb{Z}$$

where $\mathbb{Z}$ is the ring of all integers. Here we need 0 or negative integers for a or b to express $\gcd(m,n)$.

Usually the symbol '$\cdot$' for multiplication is omitted: e.g. $a \cdot m = am$.

2.4. Dirichlet's Prime Number Theorem on Arithmetic Progressions

Two integers m and n are *relatively prime* if their greatest common divisor is equal to 1; m and n are relatively prime if and only if there exist such two integers a,b as $am + bn = 1$. In the case, it is also said that n is relatively prime to m, and simply denoted as $(m,n) = 1$.

Dirichlet's Prime Number Theorem. In an arithmetic progression whose initial term and common difference are relatively prime, there appear infinitely many prime numbers. More explicitly, let d be a natural number. Then for an integer k with $(k,d) = 1$, there are infinitely many prime numbers of the form $qd + k, q \in \mathbb{N}$. We may also state that there exist infinitely many prime numbers whose residue modulo d coincide with the given residue k modulo d if $(k,d) = 1$.

3. The Ring of Integers

3.1. The Ring of Integers

The ring of integers $\mathbb{Z} = \{\ldots, -3, -2, -1, 0, 1, 2, 3, \ldots\}$ is associative and commutative. The notion of divisibility is naturally extended to integers; for two integers m and n we say that m divides n or n is divisible by m, and denote $m | n$, if $n = qm$ for some $q \in \mathbb{Z}$.

The ring $\mathbb{Z}$ is a *principal ideal domain*. An *ideal* M of $\mathbb{Z}$ is a $\mathbb{Z}$-submodule of $\mathbb{Z}$; it is an additive subgroup of $\mathbb{Z}$. Conversely, an additive subgroup of $\mathbb{Z}$ automatically becomes a $\mathbb{Z}$-module. For an ideal M of $\mathbb{Z}$, there exists such an element $d \in M$ as $M = d\mathbb{Z} = \{ad \mid a \in \mathbb{Z}\}$. A typical example of an ideal of $\mathbb{Z}$ is defined by two integers $m, n \in \mathbb{Z}$ as $M = \{am + bn \mid a, b \in \mathbb{Z}\}$. In the case, we have $M = d\mathbb{Z}$ with $d = \gcd(m,n)$.

3.2. Linear Equations in Integers and Divisibility

A linear equation of one variable X in integers is given by integers m and n as

$$mX = n;$$

this is to be solved by an integer value of X. Hence it is nothing but to ask whether n is divisible by m or not.

Let $X_1, \ldots, X_j$ be independent j variables and suppose that $m_1, \ldots, m_j, n \in \mathbb{Z}$ are given. The problem is now to find integral solutions of the linear equation

$$m_1X_1 + \cdots + m_jX_j = n.$$

This is also reduced to the problem of divisibility of n by the greatest common divisor d of $m_1,\ldots,m_j$. Indeed, put

$$M := \{a_1m_1 + \cdots + a_jm_j \mid a_1,\ldots,a_j \in \mathbb{Z}\}.$$

Then M is an ideal of the ring $\mathbb{Z}$. The problem is whether n belongs to M or not. There exists $d \in \mathbb{Z}$ so that we have $M = d\,\mathbb{Z}$. Then $d = \gcd(m_1,\ldots,m_j)$. Hence $n \in M$ if and only if $d \mid n$.

3.3. Multiplicative Structure of the Integral Solutions of Pell's Equations

An equation of the form

$$X^2 - DY^2 = 1$$

for $D \in \mathbb{N}$ is called *Pell's equation*; it is to be solved by pairs of integers for X and Y. Euler erroneously put the name of the mathematician John Pell (1611–85) although Pell did not work on such equations. Since then, however, the term 'Pell's equation' is commonly used. If D is a square, then it has only trivial solutions $(X,Y) = (\pm 1, 0)$. Suppose that D is not a square, or even that D does not have any square factors because they may be absorbed by Y. Then there always exist infinitely many integral solutions. Indeed, there is an irrational number $\varepsilon = x + y\sqrt{D}$ with $x, y \in \mathbb{Z}$ which produces all the positive integral solutions (x_n, y_n) determined by $\varepsilon^n = x_n + y_n\sqrt{D}, n = 1, 2, 3, \ldots$

Examples of ε. Here ε_0 corresponds to the smallest positive integral solution of the equation $X^2 - DY^2 = -1$ if it exists; in that case, $\varepsilon = \varepsilon_0^2$.

1. $D = 2$: $\varepsilon = 3 + 2\sqrt{2}, \varepsilon^2 = 17 + 12\sqrt{2}, \varepsilon^3 = 99 + 70\sqrt{2}; \varepsilon_0 = 1 + \sqrt{2}$.

2. $D = 3$: $\varepsilon = 2 + \sqrt{3}, \varepsilon^2 = 7 + 4\sqrt{3}, \varepsilon^3 = 26 + 15\sqrt{3}$.

3. $D = 5$: $\begin{array}{l} \varepsilon = 9 + 4\sqrt{5}, \varepsilon^2 = 161 + 72\sqrt{5}, \\ \varepsilon^3 = 2889 + 1292\sqrt{5}; \varepsilon_0 = 2 + \sqrt{5} \end{array}$.

4. $D = 6$: $\varepsilon = 5 + 2\sqrt{6}, \varepsilon^2 = 49 + 20\sqrt{6}, \varepsilon^3 = 485 + 198\sqrt{6}$.

5. $D = 7$: $\varepsilon = 8 + 3\sqrt{7}, \varepsilon^2 = 127 + 48\sqrt{7}, \varepsilon^3 = 2024 + 765\sqrt{7}$.

There appear irregular D's for which the smallest solutions are large:

6. $D = 29$: $\varepsilon = 9801 + 1820\sqrt{29}, \varepsilon_0 = 70 + 13\sqrt{29}$;

7. $D = 31$: $\varepsilon = 1520 + 273\sqrt{31}$;

8. $D = 43$: $\varepsilon = 3182 + 531\sqrt{43}$;

9. $D = 46$: $\varepsilon = 24335 + 3588\sqrt{46}$;
10*. $D = 47$: $\varepsilon = 48 + 7\sqrt{47}$;
11. $D = 53$: $\varepsilon = 66249 + 9100\sqrt{53}$; $\varepsilon_0 = 182 + 25\sqrt{53}$;
12. $D = 61$: $\begin{matrix} \varepsilon = 1766319049 + 226153980\sqrt{61}; \\ \varepsilon_0 = 29718 + 3805\sqrt{61} \end{matrix}$;
13*. $D = 62$: $\varepsilon = 63 + 8\sqrt{62}$.

In ancient Greece, integral solutions of $X^2 - DY^2 = 1$ were used to approximate the quadratic irrational number $\sqrt{D}$. Indeed, the equation $D = (X/Y)^2 - (1/Y)^2$ shows that an integral solution X and Y provide a good approximation X/Y of $\sqrt{D}$ if Y is large. In the case of $D = 2$, the second solution gives $17/12 = 1.4166\ldots$., the third $99/70 = 1.1414285\ldots$ and the fourth $577/408 = 1.41421456\ldots$ for $\sqrt{2} = 1.41421356\ldots$

-
-
-

Bibliography

Borevich, Zi.I. and Shafarevich, I. (1966). \textit{Number Theory}, Acad. Press, New York. [This book is written for the students in mathematics to give a view of the theory of numbers, of the problems with which this theory deals and of the methods that are used.]

Cohn, Harvey (1988). \textit{A classical invitation to algebraic numbers and class fields} (Universitext), Springer-Verlag. ISBN 0-387-90345-3. [This book is intended to serve both the committed number theorist and the casual but curious outsider by displaying the most significant historical steps of modern number theory.]

Gras, Georges (2003). \textit{Class field theory: from theory to practice}, Springer-Verlag, Berlin/New York. ISBN 3-540-44133-6. [This book aims to help students and researchers who are familiar with classical algebraic number theory in the practical use and understanding of the principles of global class field theory for number fields.]

Koch, Helmut (2000). *Number Theory : Algebraic Numbers and Functions*, xviii+368 pp. Graduate Studies in Mathematics Volume 24, Amer. Math. Soc., Providence, RI, ISBN 0-8218-2054-0.[This book is an excellent and well organized introduction of number theory.]

Washington, Lawrence (1999). \textit{Introduction to cyclotomic fields}, Graduate Textes in Math. 83, Springer-Verlag, third edition. ISBN 3-540-94762-0. [This is a well prepared introduction to the modern cyclotomy and the Iwasawa theory.]

Weil, André (1984). *Number Theory : an approach through history from Hammrapi to Legendre*, Birkhäuser, Boston, ISBN 0-8176-3141-0 3-7643-3141-0.[This is an exceptional exposition of the origins of modern number theory up to the end of the 18th century.]

Biographical Sketch

Katsuya MIYAKE born 1941 in Hyogo-Ken, Japan
Education: BS in Mathematics, Tokyo University, Japan (March, 1964). MS in Mathematics, Tokyo University, Japan (March, 1966). Ph.D. in Mathematics, Princeton University, U.S.A. (June, 1969).
Positions held: Researcher, Courant Institute for Mathematical Sciences, New York University, U.S.A. (September, 1969--August, 1970), Assistant Professor, Department of Mathematics, Nagoya University, Japan (September, 1970--December, 1973), Associate Professor, Department of Mathematics, Nagoya University, Japan (January, 1974--August, 1986), Professor, Department of Mathematics, Nagoya University, Japan (September, 1986--March, 1993), Professor, Department of Mathematics, Tokyo Metropolitan University, Japan (April, 1993--March, 2005), Professor Emeritus, Tokyo Metropolitan University (April, 2005 to date), Visiting Professor, Department of Mathematics, Waseda University, Japan (April, 2005 to date), Visiting Professor, Institute for Mathematics and Computer Science, Tsuda College, Japan (April, 2005 to date).