About Number Theory

Some basic results with applications to physics

Introduction

Charles Widger 6 Mar 2025

Some Beginning References

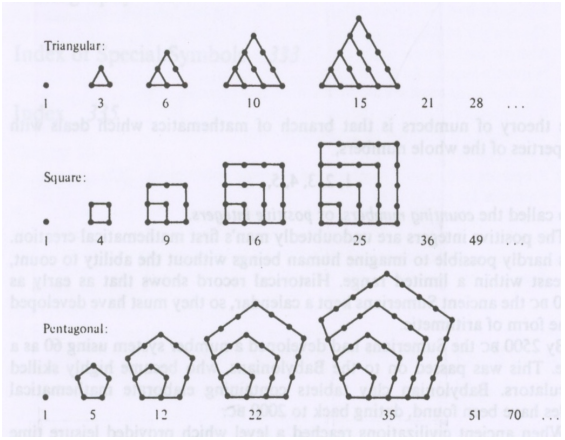
For those of modest mathematical background

- **Introduction to the Theory of Numbers**
  - Leonard Eugene Dickson (1874-1954), 1929, University of Chicago, Dover Edition 1957
- **An Introduction to the Theory of Numbers**
  - Ivan Niven (1915-1999) and Herbert Zuckerman (1912-1970), 1960, John Wiley & Sons
    - Zuckerman translated **Von Zahlen und Figuren; proben mathematischen Denkens für Liebhaber der Mathematik** by Hans Rademacher and Otto Toeplitz (1933) with an addendum of 2 chapters as **The Enjoyment of Mathematics** (1957) Princeton University Press. I audited his class in Number Theory in 1963. He also had a 30+ page mimeographed list of intriguing mathematical materials.
- **Introduction to Analytic Number Theory**
  - Tom Apostol (1923-2016), 1976, Springer Science+Business Media
    - Tom Apostol attended the University of Washington for his BS and MS degrees. He probably came under the influence of Herbert Zuckerman while studying there. Those two coauthored two papers.
- **Number Theory in Science and Communication**
  - Manfred R. Schroeder (1926-2009), 2009, Springer-Verlag, 5th edition
    - The author is a Ph.D. physicist who was influenced by a talk on number theory given at Göttingen by André Weil (1906 - 1998).

Historical Background

A very short, incomplete, overview

- Sumerians
  - Developed a calendar around 3,500 BCE
  - Developed a counting system by 2,500 BCE using base 60.
- Babylonians
  - Developed mathematical tables, dating back to 2,000 BCE
- Mayans
  - Developed a base 20 counting system in use by 1000 BCE.
  - Developed a symbol for zero. It is used on monuments dated at 357 AD.
  - Developed calendar with a more accurate yearly earth rotation around the sun than that for our current Gregorian calendar.
- Greeks
  - Systematic developments in numbers and geometry, including the two together. Pythagorus around 600 BCE, Euclid around 300 BCE, Diophantus of Alexandria around 250 AD. NB: The Romans burnt the library of Alexandria in 48 BCE.
- Hindis, Chinese, Arabs active
- Italians and French
  - Fibonacci (c. 1170 - c. 1250) popularized use of the Indu-Arabic numeral system.
  - Pierre de Fermat (1601 - 1665), considered the father of modern number theory, found:
    - Every positive integer is either a triangular number or a sum of 2 or 3 triangular numbers
    - Every positive integer is either a square or a sum of 2, 3, or 4 squares
    - Every positive integer is either a pentagonal number or the sum of 2, 3, 4, or 5 pentagonal numbers



Classification of numbers by geometry

Getting Started

Definitions & Notations

- Define the natural numbers $\mathbb{N}$ as in Wikipedia under the article for the Peano Axioms.
  - Adopt the notations used in this article.
    - Warning: the article uses a function $\varphi(n)$ as a unary predicate. We will have a second use of this symbol, due to Euler. The meaning should be apparent from the context in which it appears, The set of natural numbers is an ordered semiring $(\mathbb{N}, +, \cdot, 1, 0, \leq)$.
- We will regard a number as something different than a representation of a number, which we will call a *numeral*. So the number corresponding to 2 is S(S(0)), where S is the successor function of the Peano axioms. Alternate ways of writing it include with Roman numerals: II, or in Chinese: 二, or spelled out in German: zwei.
- The multiplication operator is binary. Its domain entries are called factors. The result is the product. The factors are divisors of the product. So, a divides b if there is a number k such that $ak = b$. We also write $a \mid b$. If there is no such number k, we write $a \nmid b$. If a number has at least two divisors, neither being 1, it is said to be *composite*.
- A number c is a common divisor of numbers a and b provided both $c \mid a$ and $c \mid b$. If one of a or b is not 0, the pair has a common divisor. The largest of these common divisors is called the greatest common divisor, and is denoted by $\gcd(a, b)$, but also just the ordered pair, *(a,b)* is used.
- A number $c > 0$ is a common multiple of numbers $a > 0$ and $b > 0$, provided both $a \mid c$ and $b \mid c$. Note the product of a and b is such a number. The *least common multiple* is minimum of the set of common multiples and is denoted as $\operatorname{lcm}(a,b)$. It can determine how often Mercury, Venus and Earth are in syzygy.
- A natural number n is *prime* if and only if it has no divisor d such that $1 < d < n$. We denote the set of prime numbers as $\mathbb{P}$. If two numbers have gcd = 1, they are said to be coprime.

About Lattices

An Aside

- A *lattice* is a partially ordered set (*poset*) L with with two binary operators called *join*, denoted by $\vee$, and *meet*, denoted by $\wedge$. Further, these operators satisfy these two *absorption laws*: $a \vee (a \wedge b) = a$ and $a \wedge (a \vee b) = a$. In consequence thereof, they also satisfy the *idempotent laws*, $a \vee a = a$ and $a \wedge a = a$.
- A bounded lattice is a lattice that has a *greatest element* (also called a *maximum* or *top element*, denoted by 1 or $\top$) and a *least element* (also called a *minimum* or a *bottom element*, denoted by 0 or $\bot$).
- Examples of lattices:
- Examples of non-lattices:

On Primes

Some basic facts

- Theorem: Given any prime number p, there is a prime number q such that $p < q$.
  - Consider the set $\{p_i, 1 \leq i \leq n\}$, where p_i is prime, $p_i < p_{i+1}$, and $p_n = p$. Then set $q = 1 + \prod_{i=1}^{n} p_i$. If q is prime, we are done because it is greater than p. If q is composite, no factor of q can be smaller or equal to p. This proof is attributed to Euclid.
  - Corollary: There are an infinite number of primes.
- Theorem: There are arbitrarily large gaps in the sequence of primes. In other words, if k is a natural number, there is a sequence of k consecutive composite numbers.
  - Consider the numbers $(k + 1)! + j$, for all j, $2 \leq j \leq k + 1$. The number j divides each of these numbers.

A bit more on primes

Factoring into primes is unique

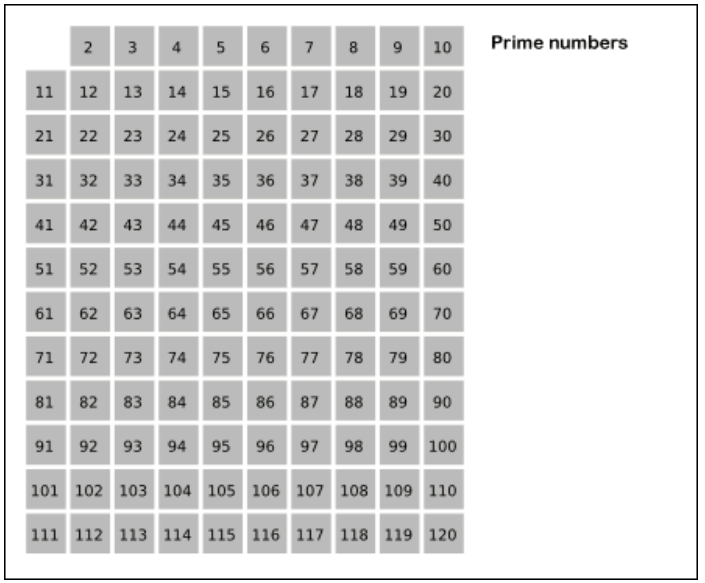
- Fundamental Theorem of Arithmetic: The factoring of any positive natural number is unique apart from the order of the primes.
  - Lemma: If $p \mid ab$, where p is prime, then $p \mid a$ or $p \mid b$. More generally, if $p \mid \prod_{i=1}^{N} a_i$, then p divides at least one factor of the product.
    - If $p \nmid a$, the gcd(p, a) = 1. So $p \mid b$.
  - Proof of Theorem: Divide out all the common prime factors to get some number, Q, which has two different factorings as primes, say $\prod_{i=1}^{r} p_i = \prod_{i=1}^{s} q_i$. Then $p_1 \mid \prod_{i=1}^{s} q_i$ and so by the lemma, p_1 divides one of the q_i $1 \leq i \leq s$. This contradicts the assumption that all the common factors have been divided out.

Finding Prime Numbers

Prime number generation and Tests for Primality

- Generation
  - Sieves
    - Eratosthenes (250 BCE), Sundaram (1934), Pritchard (1979), Atkin (2003),
  - Special subsets, such as the Mersenne numbers
- Tests
  - Trial Division: It has a lengthy process. It took some time to see one only needs trials up to $\lfloor \sqrt{n} \rfloor$, where n is the number being investigated. The floor function yields the largest integer less than the argument.
  - Miller-Rabin: This is reasonably fast, but it may give a false result.
  - Agrawal-Kayal-Saxena (AKS): This always gives a correct result, but is too slow to be practical.
  - Wilson's theorem: More on this, after we speak to congruence. Too complex computationally for much use.
  - Tests for Mersenne numbers: These are numbers of the form $M_n = 2^n - 1$. Sometimes n is required to be prime. As of 2024, 52 Mersenne primes are known. The largest known is for n = 136,279,841. It has 41,024,320 digits.

Sieve of Eratosthenes



About Division

Two Algorithms

- The Division Algorithm:
  - Given integers a and b with $b > 0$, there is a unique pair of integers q and r such that $a = bq + r$, with $0 \leq r < b$. Furthermore, $r = 0$ if, and only if, $b|a$. We say q is the *quotient* and r is the *remainder* when b is divided into a.
    - Let S be the set given by $S = \{ y : y = a - bx, x \text{ is an integer}, y \geq 0\}$. This is a non-empty set of non-negative integers, so it has a smallest member, say $a - qb$. Define r by $r = a - qb$. Then $a = qb + r$ and $r \geq 0$. Next, we show $r < b$. Assume the opposite, $r \geq b$. Then $0 \leq r - b < r$. Then $(r - b) \in S$ since $r - b = a - b(q + 1)$. This contradicts r being the smallest in S. A similar argument shows the pair q and r are unique.
- The Euclidean Algorithm:
  - Given positive integers a and b, where $b \nmid a$. Let $r_0 = a$, $r_1 = b$, and apply the division algorithm to define a set of remainders $r_0 = r_1q_1 + r_2$, $r_1 = r_2q_2 + r_3$, ..., $r_{n-2} = r_{n-1}q_{n-1} + r_n$. Note than for each step, $r_n < r_{n-1} < ... < r_0$. Since these are monotonic decreasing, there will be some n for which $r_{n+1} = 0$. The last non-zero remainder is the gcd of a and b.
    - Example: $a = 1071$, $b = 462$. 1st Step: $1071 = 2 \times 462 + 147$. 2nd Step: $462 = 3 \times 147 + 21$. 3rd Step: $147 = 7 \times 21 + 0$. Thus gcd (1071, 262) = 21.

Some sums of natural numbers

Reciprocals of primes

- Theorems: The sum of the reciprocals of the natural numbers; *id est*, the harmonic series, diverges. If one restricts the reciprocals to only those that are perfect squares, then the sum converges.
- Theorem: Let $s_n = \sum_{k=1}^{n} 1/p_k$, where p_k is the sequence of prime numbers. Then $\lim_{n\to\infty} s_n = \infty$. This was proved by Euler.
- On the other hand, if one includes only twin primes, like 3 and 5, 5 and 7, and 11 and 13, then the result converges. This was proved in 1919 by Viggo Brun (1885 - 1978), a Norwegian mathematician. The sum is defined to be $B_2 = \sum_{p \wedge p+2 \in \mathbb{P}} (\frac{1}{p} + \frac{1}{p+2})$. The subscript on B indicates pairs of primes are being taken. Groupings of 4 consecutive primes have also been considered, and these sums converge to a B_4. The values of B_2 and B_4 are not known, but B_2 is thought to be around 1.9. It is yet unknown whether the set of twin primes is finite.

Congruence

Modular Numbers

- Given a natural number $m \geq 1$, two integers *a* and *b* are said to be *congruent modulo m* if and only if m divides their difference; *id est*, there is an integer *k* such that *a* - *b* = *km*. When *a* and *b* are congruent modulo *m*, we write $a \equiv b \pmod{m}$.
  - Note: $-1 \equiv m - 1 \pmod{m}$
  - Congruence is an *equivalence relation* because it is *reflective* because $a \equiv a \pmod{m}$, it is *symmetric* because $a \equiv b \pmod{m}$ implies $b \equiv a \pmod{m}$, and *transitive* because {if $a \equiv b \pmod{m}$ and $b \equiv c \pmod{m}$} then $a \equiv c \pmod{m}$.
  - A number *g* is a *primative root modulo n* if for every integer *a* coprime to *n*, there is some integer *k* for which $g^k \equiv a \pmod{n}$.
- The set of integers congruent modulo *m* can be represented by {*0, 1, ... m-1*}. It is called a **complete residue system modulo *m***. A member *a* of this set may be represented by $\bar{a}_m$.
- Define addition and multiplication as with integers and reduce the sum and product modulo *m*. For example, $\overline{12}_{24} + \overline{21}_{24} = \overline{33}_{24} = \overline{9}_{24}$. So defined, a complete residue system modulo *m* is a ring. It also inherits the order relation. Denote this ring by $\mathbb{Z}/m\mathbb{Z}$. It is the quotient ring of $\mathbb{Z}$ by the ideal $m\mathbb{Z}$, the set of integers that are multiples of *m*. This quotient ring is a field if and only if *m* is prime.
- Applications of these modular numbers beyond number theory include group theory, ring theory, knot theory, abstract algebra, computer algebra, cryptography, computer science, chemistry, and the visual and musical arts.

Useful Definitions

- Two integers are *relatively prime* if and only if their gcd is 1. Two such integers are also said to be *prime to each other*.
- The *Euler totient function* ϕ at natural number $m > 0$ has value equal to the number of natural numbers not exceeding m which are relatively prime to m. The term *totient* was coined by James Joseph Sylvester (1814-1897).
- Examples:

m:	1	2	3	4	5	6	7	8	9	10
$\varphi(m)$:	1	1	2	2	4	2	6	4	6	4

About Chinese

Preparation for what comes next

- A British diplomat Thomas Francis Wade invented a romanization of Mandarin, the dialect spoken around Beijing, so one could read this text and pronounce the words correctly. It was published in 1867. An improvement was made by Herbert Giles in 1892. This work became the standard for people speaking English and has been used for several decades. In Wade-Giles, Beijing is spelled Peking. The pronunciation is the same. Mandarin is a much newer than other Chinese dialects. Chinese writing does not reveal pronunciation, but rather expresses meaning as an ideograph, as indo-arabic numerals do. For example, 火 is fire (imagine flames), 車 is cart, and 火車 is a train.
- The Chinese invented other methods. The famous geometer, Shiing-Shen Chern (1911-2004) used Gwoyeu Romatzyh defined about 1924, for his name in English. In speaking English, he would say, churn. In Mandarin, he would say Chen^{2}.
- During World War II, the USA sent many personnel to China to carry on operations. The Wade-Giles romanization takes some training to use. The military wanted something simpler, and Yale University professors were tasked to gin one up. They ginned up two, one for Mandarin, the other for Cantonese. These are known as the Yale methods. They were quiet successful.
- After Mao Tse Tung won the civil war in 1948, he wanted an official Chinese method. It is a variant on the Yale method for Mandarin. It is called pinyin. We will use it. It is official in the People's Republic of China and in Singapore.
- Chinese is tonal language. Basically, one sings the words. Mandarin has 4 different tones, *flat*, *rising*, *down and then up*, and *descending*. One way to denote which to use is by superscript. Ma^{1} ma^{1} ma^{4} ma^{3} means: Mother scolds the horse. Another way is to diacritic marks above the vowel: macon, acute accent, caron, and grave accent. Thus *mā má mǎ mà* for all 4 tones.

Some Results Involving Primes

- **Fermat's Little Theorem**: Let p be a prime and b a natural number. If $p \nmid b$ then $b^{p-1} \equiv 1 \pmod{p}$.
- **Euler's generalization of Fermat's Little Theorem**: If $p \nmid b$, then $b^{\phi(m)} \equiv 1 \pmod{m}$.
- **Wilson's Theorem**: If p is prime, then $(p-1)! \equiv -1 \pmod{p}$.
- **Chinese Remainder Theorem**: Let $\{m_i, 1 \leq I \leq r\}$ be r positive integers that are relative prime in pairs, and let $\{a_i, 1 \leq i \leq r\}$ be a set of r integers. Then, the set of congruences $x \equiv a_i \pmod{m_i}$ for $1 \leq i \leq r$ have common solutions. Any two solutions are congruent modulo $\prod_{i=1}^{r} m_i$.
  - From Sūnzǐ Suànjīng (孫子算經), written during 3rd to 5th centuries of the CE. Posed there as a problem: We have some number of things. If we group them by threes, we have 2 left over. If we group them by fives, we have 3 left over. If we group them by sevens, we have 2 left over. How many do we have?
  - General case stated and proved by Qín Jiǔsháo (秦九韶) in 1247.
  - This is used in most RSA encryption applications during signing of HTTPS certificates and during decryptions.
- **Bertrand's Postulate**: For every positive integer $n > 1$, there is a prime p such that $n < p \leq 2n$. Conjectured by Joseph Bertrand (1822 - 1900) in 1848, proved by Pafnuty Chebyshev (1821 - 1894) in 1852.

More on Number Theory

Part 2

Charles Widger, 25 Feb 2025

Review from Introduction

Preparation for more on the Chinese Remainder Theorem

- Given a natural number $m \geq 1$, two integers a and b are said to be *congruent modulo m* if and only if m divides their difference; *id est*, there is an integer k such that $a - b = km$. When a and b are congruent modulo m, we write $a \equiv b \pmod{m}$.
  - Note: $-1 \equiv m - 1 \pmod{m}$
  - A number g is a *primative root modulo n* if for every integer a coprime to n, there is some integer k for which $g^k \equiv a \pmod{n}$; k is called the *index* or *discrete logarithm of a to base g modulo n*.
    - Example: 3 is a primitive root modulo 7.
- **Chinese Remainder Theorem**: Let $\{m_i, 1 \leq I \leq r\}$ be r positive integers that are relative prime in pairs, and let $\{a_i, 1 \leq i \leq r\}$ be a set of r integers. Then, the set of congruences $x \equiv a_i \pmod{m_i}$ for $1 \leq i \leq r$ have common solutions. Any two solutions are congruent modulo $M = \prod_{i=1}^{r} m_i$.
  - From Sūnzǐ Suànjīng (孫子算經), written during 3rd to 5th centuries of the CE. Posed there as a problem: We have some number of things. If we group them by threes, we have 2 left over. If we group them by fives, we have 3 left over. If we group them by sevens, we have 2 left over. How many do we have?

Chinese Remainder Theorem

As proved in Niven & Zuckerman

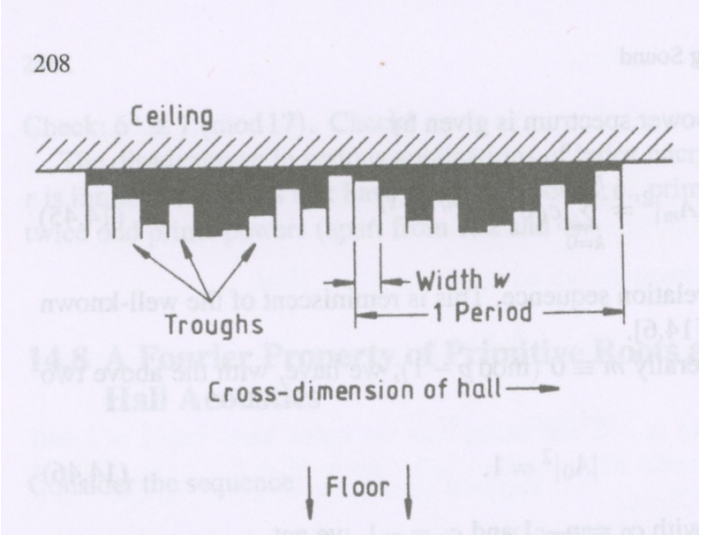
- We have a set of congruences $x \equiv a_i \pmod{m_i}$ for $1 \leq i \leq r$, where the each pair of m_i with m_j $i \neq j$ are relatively prime; that is, they share no prime factors.
- Set $M = \prod_{i=1}^{r} m_i$. Then $\frac{M}{m_i}$ is an integer and $\gcd(M/m_i, m_i) = 1$. Thus there are integers b_i $1 \leq i \leq r$ such that $(M/m_i)b_i \equiv 1 \pmod{m_i}$. But, $(M/m_i)b_i \equiv 0 \pmod{m_j}$ when $i \neq j$. Define $x = \sum_{i=1}^{r} (M/m_i)b_i a_i$. Then $x \equiv \sum_{i=1}^{r} \frac{M}{m_i} b_i a_i \pmod{m_i} \equiv a_i \pmod{m_i}$. That is, x is the common solution to the equations. If x and y are both common solutions, then $x \equiv y \pmod{M}$. This completes the proof.

- For the case in 孫子算經, note the elements of the set $\{3, 5, 7\}$ is relatively prime by pairs. Define $a_1 = 2$, $a_2 = 3$, and $a_3 = 2$. Further, define $m_1 = 3$, $m_2 = 5$, $m_3 = 7$, and $M = m_1 m_2 m_3 = 105$. Then $M/m_1 = 35$, $M/m_2 = 21$, $M/m_3 = 15$. Note $M/m_1 = 35 \equiv 2 \pmod{3}$, $M/m_2 = 21 \equiv 1 \pmod{5}$, and $M/m_3 = 15 \equiv 1 \pmod{7}$. Let $b_1 = 2$, $b_2 = 1$, $b_3 = 1$.
  - Then $(M/m_1)b_1a_1 = 140 \equiv 2 \pmod{3}$, $(M/m_2)b_2a_2 = 63 \equiv 3 \pmod{5}$, and $(M/m_3)b_3a_3 = 30 \equiv 2 \pmod{7}$. So the equations are solved.
  - Further, the solutions are of the form: $x = (1 + 21 + 1) + 105k = 23 + 105k$, k is an integer. Compare with Wikipedia, here.

Application of Chinese Remainder Theorem

Concert Hall Acoustics, Introduction

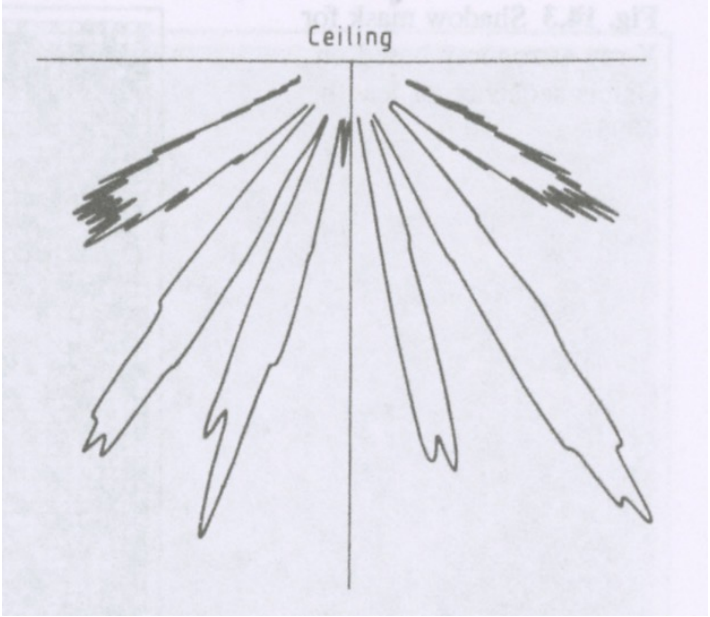
- Discussed in book by Schroeder, Section 14.9, pp. 207-209
- Halls with laterally traveling sound waves have better sound than those with short-path sound arriving only from the front.
- The short-path sounds are typical for halls with a low ceiling. Construction costs and building codes are restrictions on design.
- Sound reflected from a hard surface ceiling has varying intensities of peaks and throughs.
- Schroeder suggested mounting reflection phase-gratings on the ceilings that scatter sound intensities in all diffraction directions except straight down.



Concert Hall Acoustics

Continuation

- Recall a number *g* is a *primitive root modulo n* if every number *a*, *coprime to n*, is congruent to a power of *g* modulo *n*.
- Construct a reflection phase-grating with wells of different depths d_n, which change the phase of a normally incident wave of length λ by $2d_n 2\pi/\lambda$. Choose the $d_n = \frac{1}{2}\frac{\lambda g^n}{p}$, where g is a primitive root of the prime p. In this way, the reflective wave has complex amplitude given by $a_n = e^{2\pi i g^n/p}$. The prime *p* must be chosen so that *p-1* has two coprime factors. For example, for $p = 11$, $p - 1 = 10 = 2 \times 5$. This yields 10 numbers, $\{a_i , 1 \leq i \leq 10\}$, thought of as the remainders in the Chinese Remainder Theorem, which can fill a 2 by 5 array to construct the phase-grating.
- The illustration shows such an array with backscatter measured.



Specialized Functions

Beyond the Euler Totient

- To say that there is a laundry list of functions used in number theory is an understatement. Here is a listing of a bunch:
  - The pi function, $\pi(x)$ = the number of primes p satisfying $2 \leq p \leq x$.
  - Bernoulli polynomials and the Bernoulli periodic function; Chebyshev $\psi(x)$ and $\theta(x)$; Dirichlet $L(s,\chi)$; a series of divisor functions $\sigma_\alpha(n)$; Hurwitz zeta $\zeta(s,a)$, which generalizes Riemann zeta $\zeta(s)$; Liouville $\lambda(n)$; Mangoldt $\Lambda(n)$; Möbius $\mu(n)$; $d(n)$, $\nu(n)$, $\kappa(n)$, $M(x)$, and $\psi_1(x)$.
    - Several of these, such as the Euler Totient and Möbius μ have the property of being multiplicative; a function f is multiplicative if $f(mn) = f(m)f(n)$.

Prime Number Theorem

Establishes a bound on the growth of numbers of primes

- A concise statement is: $\lim_{x \to \infty} \frac{\pi(x) \log x}{x} = 1.$
- Proved in 1896 by Jacques Hadamard (1865 - 1963) and independently by baron Charles Jean de Vallée Poussin (1866 - 1962).
- The proof in book by Niven and Zuckerman uses continued fractions.
- The proof in book by Apostol uses mathematical analysis.

Diophantine equations

Equations with integer solutions

In the following equations, w, x, y, and z are the unknowns and the other letters are given constants

$ax + by = c$

Linear, related to the identity of Bézout (1730 - 1783)

$w^3 + x^3 = y^3 + z^3$

The smallest nontrivial solution in positive integers is $12^3 + 1^3 = 9^3 + 10^3 = 1729$. It was famously given as an evident property of 1729, the number of a taxicab, hailed by Ramanujan (1887 - 1930) and Hardy (1877 - 1947) while meeting in 1917. There are infinitely many nontrivial solutions.

$x^2 - ny^2 = \pm 1$

This is Pell's equation, which is named after the English mathematician John Pell (1611 - 1685). It was studied by Brahmagupta (c. 598 - c. 668 CE) in the 7th century, as well as by Fermat in the 17th century.

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

The Erdös-Straus conjecture states that, for every positive integer n ≥ 2, there exists a solution in x, y, and z, all as positive integers. Although not usually stated in polynomial form, this example is equivalent to the polynomial equation 4xyz = n(yz + xz + xy).

$x^4 + y^4 + z^4 = w^4$

Conjectured incorrectly by Euler to have no nontrivial solutions. Proved by Noam Elkies to have infinitely many nontrivial solutions. A computer search by Roger E. Frye determined the smallest nontrivial solution is

$95{,}800^4 + 217{,}519^4 + 414{,}560^4 = 442{,}481^4$

Fermat's Last Theorem

A very famous Diophantine equation

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

For n = 2, there are infinitely many solutions (x, y, z): the Pythagorean triples. For larger integer values of n, Fermat stated in 1637 that there are no positive integer solutions (x, y, z). Other statements by him were deemed theorems, but this one had a while to wait.

- That the statement is true for n = 4 was proved later by Fermat. This case is an exercise in the reference book by Dickson.
- Considerable effort over the next 358 years eventually led to a published proof of correctness by Andrew Wiles in 1997.
  - Up to 1839, so two centuries later, it had been established as true for the primes 3, 5, and 7.
  - Marie Sophie Germain (1776 - 1831) established a theorem that bears her name as published by Adrien-Marie Legendre in 1823. He had used this to establish Fermat's theorem for n = 5. Leonard E. Dickson, author of reference 1, above, used this theorem to establish Fermat's theorem for all odd primes less than 1700.
- More progress was obtained especially with the application of the modern algebra and ring theory by Richard Dedekind and his work on ideals.
- An even more modern development was the application of computers. By 1954, Fermat's conjecture was shown to be correct for n being a prime number less than 2,521. By 1993, it was extended to all primes less than 4 million.
- Wiles innovation was to restate the problem in terms of elliptic curves as defined in the study of differential geometry. His methods not only settled Fermat's Last Theorem, they addressed the Taniyama–Shimura–Weil conjecture regarding elliptic curves as well.

Quadratic Residues

On the equation $x^2 \equiv a \pmod{m}$

- For all a and m such that gcd(*a*,*m*) = 1, *a* is said to be a *quadratic residue modulo m* if the congruence given has a solution. If it does not have a solution, it is said to be a *quadratic non-residue modulo m*.
- For *p* an odd prime and *a* an integer relatively prime to *p*, the Legendre symbol $\left(\frac{a}{p}\right)$ is defined to be 1 if *a* is a quadratic residue modulo *p*, and -1 if *a* is a quadratic non-residue modulo *p*.
- Let *p* be an odd prime, and *a* and *b* be integers relatively prime to *p*. Then:
  - $\left(\frac{a}{p}\right) \equiv a^{(p-1)/2} \pmod{p}$
  - $\left(\frac{a}{p}\right)\left(\frac{b}{p}\right) = \left(\frac{ab}{p}\right)$
  - $a \equiv b \pmod{p}$ implies $\left(\frac{a}{p}\right) = \left(\frac{b}{p}\right)$
  - $\left(\frac{a^2}{p}\right) = 1$, $\left(\frac{1}{p}\right) = 1$, and $\left(\frac{-1}{p}\right) = (-1)^{(p-1)/2}$

Partitions

Switch from studying multiplication to addition

- Basic problem: Given a set A = $\{a_i, 1 \leq i \leq \infty\}$, where the a_i are special in some way, such as being primes, squares, cubes, triangular numbers, *etc*. Each representation of n as a sum of elements in A is called a *partition* of n. We are interested in a function $A(n)$, which counts the number of partitions of n into summands from A.
- In 1742, Christian Goldbach conjectured: Every even $n > 4$ is the sum of two odd primes.
  - Here, A(n) is the number of solutions of $n = p_1 + p_2$, where p_1 and p_2 are odd primes. This conjecture remains undecided to this day. The cases of n = 6 or 8 is easy to resolve. In 1937, Ivan Matveevich Vinogradov (Ива́н Матве́евич Виногра́дов) proved every sufficiently large odd number is the sum of 3 odd primes. In 1973, Chen Jingrun (陳景潤;) showed every sufficiently large even number is the sum of a prime plus a number with no more than two prime factors.
- Consider representation by squares: For a given integer, $k \geq 2$, consider the partition function $r_k(n)$ which counts the number of solutions of the equation $n = \sum_{i=1}^{k} x_i^2$, where the x_i may be positive, negative, or zero and the order of the summands is taken into account.
  - Carl Gustav Jacob Jacobi proved that for k = 2, 4, 6, or 8 expressed $r_k(n)$ in terms of divisor functions. For example, $r_2(n) = 4[d_1(n) - d_3(n)]$, where $d_1(n)$ and $d_3(n)$ are the number of divisors of n congruent to 1 and 3 respectively. Exact formulas for k = 3, 5, and 7 have been found.
- Waring's Problem: Determine whether, for a given positive integer k, there is an integer s such that the equation $n = \sum_{i=1}^{s} x_i^k$ has solutions for every $n \geq 1$. Proved by David Hilbert in 1909.

The Partition Function

Including variations

- Definition: The partition function p maps a positive integer n into the number of distinct ways n can be written as a sum of positive integers. Two partitions are different if they have different summands. Extend the domain to include 0 by defining $p(0) = 1$.
  - $p(5) = 7$. Here they are:
    - $5 = 5$, $5 = (4+1)$, $5 = (3+2)$, $5 = (3+1+1)$, $5 = (2+2+1)$, $5 = (2+1+1+1)$, $5 = (1+1+1+1+1)$.
  - There is also a raft of variations on the partition function: $p_m(n)$ = the number of partitions into summands less than or equal to m; $p^o(n)$ = the number of partitions of n into odd summands; $p^d(n)$ = the number of partitions of n into distinct summands; $q^e(n)$ = the number of partitions of n into an even number of distinct summands; $q^o(n)$ = the number of partitions of n into an odd number of distinct summands.
    - Some relations between these are easy to derive:
      - a) $p_m(n) = p(n)$ if $n \leq m$;
      - b) $p_m(n) \leq p(n)$ for all $n \geq 0$;
      - c) $p_m(n) = p_{m-1}(n) + p_m(n - m)$ if $n \geq m > 1$;
      - d) $p^d(n) = q^e(n) + q^o(n)$.
    - For $n \geq 1$, $p^d(n) = p^o(n)$ is a bit harder to establish, but true nonetheless.

A Theorem of Euler

Example of a Dirichlet Series

- Euler proved that for |x| < 1, $\prod_{i=1}^{\infty} \frac{1}{(1-x^i)} = \sum_{n=0}^{\infty} p(n)x^n$.
- A function F defined by a *Dirichlet* series for complex *s*, $F(s) = \sum_{n=1}^{\infty} f(n)n^{-s}$ is said to be a *generating function* of the coefficients *f(n)*.

Generating function	The number of partitions of *n* into parts which are
$\prod_{m=1}^{\infty} \frac{1}{1-x^{2m-1}}$	odd
$\prod_{m=1}^{\infty} \frac{1}{1-x^{2m}}$	even
$\prod_{m=1}^{\infty} \frac{1}{1-x^{m^2}}$	squares
$\prod_{p} \frac{1}{1-x^{p}}$	primes
$\prod_{m=1}^{\infty} (1+x^m)$	unequal

Pentagonal-numbers theorem

From the Book by Apostol

- Proved by Euler.
- Consider the partition function generated by the reciprocal of the generating function *p(n)*: $\prod (1 - x^m)$.
- Write $\prod_{m=1}^{\infty} (1 - x^m) = 1 + \sum_{n=1}^{\infty} a(n)x^n$.
- Note that $a(n) = p_e(n) - p_o(n)$.

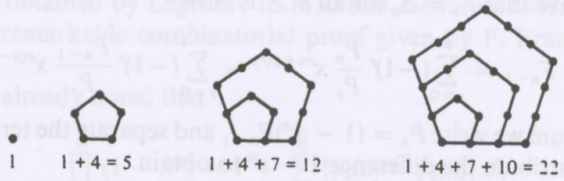


Figure 14.1

These numbers are also the partial sums of the terms in the arithmetic progression

$$1, 4, 7, 10, 13, \ldots, 3n + 1, \ldots$$

If $\omega(n)$ denotes the sum of the first n terms in this progression then

$$\omega(n) = \sum_{k=0}^{n-1} (3k + 1) = \frac{3n(n-1)}{2} + n = \frac{3n^2 - n}{2}.$$

The numbers $\omega(n)$ and $\omega(-n) = (3n^2 + n)/2$ are called the *pentagonal numbers*.

Theorem 14.3 Euler's pentagonal-number theorem. *If* $|x| < 1$ *we have*

$$\prod_{m=1}^{\infty} (1 - x^m) = 1 - x - x^2 + x^5 + x^7 - x^{12} - x^{15} + \cdots$$

$$= 1 + \sum_{n=1}^{\infty} (-1)^n \{x^{\omega(n)} + x^{\omega(-n)}\} = \sum_{n=-\infty}^{\infty} (-1)^n x^{\omega(n)}.$$

Possible Later Presentations

Depending on health and other distractions

- RSA encryption
- Error correcting codes (some fun: look at the table of contents to this book)
- The Common Criteria for security of networked systems
- Category Theory
- Time Series Statistical Analysis
- Spread Spectrum Communications
- Biography of Herbert Zuckerman