

1 INTRODUCTION TO NUMBER THEORY

University of Windsor MATH 3270 Class Notes, by M. Hlynka and W.L. Yee.
These notes are based on the text “Number Theory with Computer Applications” by Kumanduri and Romero. Large parts are taken verbatim.

Three major branches of mathematics:

- algebra
 - study of algebraic structures: groups, rings, fields, modules, vector spaces, lattices, algebras
- analysis
 - the study of how things change, local structure eg. calculus
- geometry/topology
 - study of shapes

Number theory is the study of integers

Branches of number theory: analytic and algebraic

Number Theory studies problems such as

1. Find all integer solutions to $x^n + y^n = z^n$ for $n \geq 3$ (Fermat’s last Theorem).

Fermat claimed a proof (1637) that only trivial solutions (like $0^3 + 4^3 = 4^3$) exist.

Mathematicians searched for a proof for hundreds of years.

Andrew Wiles found a complex proof (1994) that was widely celebrated.

References:

“The Simpsons”: In one show, the equation $1782^{12} + 1841^{12} = 1922^{12}$ is visible. With a calculator compute LHS and find its 12th root to get 1922.

Does this contradict Fermat’s last Theorem?

Arthur Porges, “The Devil and Simon Flag” is a mathematical version of the story “The Devil and Daniel Webster” (by Stephen Vincent Benet) which is based on the German legend Faust, but using Fermat’s last Theorem.

2. Show that $\pi(n)$, the number of primes less than or equal to n is asymptotically $\frac{n}{\ln n}$ (the Prime Number Theorem; conjectured by Gauss, 1792, proved independently by Jacques Hadamard and Charles Jean de la Vallée Poussin in 1896 using ideas introduced by Riemann, in particular the Riemann zeta function).

3. Goldbach’s Conjecture (1742) Every even integer greater than 2 can be written as the sum of two primes.

Reference: (Novel) Uncle Petros & Goldbach’s Conjecture, by Apostolos Doxiadis

Chen Jingrun proved (1973) that every large even number is the sum of two primes, or a prime and the product of two primes. A Chinese postage stamp honours him.

(<http://jeff560.tripod.com/images/chen1.jpg>)

Has been shown to hold for all integers less than 4×10^{18}

Brief History:

- earliest known evidence: Plimpton 322, 1800 BC, a Babylonian clay tablet containing Pythagorean triples; too many triples to have been computed brute force
- Pythagoreans, 500 BC: $\sqrt{2}$ is irrational
- Euclid, 300 BC: Euclid’s Elements: divisibility, primes; Euclidean algorithm for finding gcd, first known proof that there are infinitely many prime numbers
- Sunzi Suanjing, 300-500 AD: Chinese Remainder Theorem

Early Modern Number Theory:

- Fermat (1601-1665):
 - Fermat’s Little Theorem
 - every prime congruent to 1 modulo 4 can be written as $a^2 + b^2$
 - Fermat’s Last Theorem ($n = 3$ proved by Euler in 1753)
- Euler (1707-1783)
 - every integer is a sum of four squares
 - Fermat’s Last Theorem for $n = 3, 4$
 - pioneered analytic number theory
- Gauss (1777-1855)
 - law of quadratic reciprocity
 - quadratic forms
 - congruence notation
 - connecting abstract algebra to number theory

Modern Number Theory:

- complex analysis, group theory, Galois theory developed; incorporated into number theory
- two branches: analytic number theory, algebraic number theory

Some classic references in number theory are:

- Andrews, G.E. (1994). Number Theory, Dover.
- Hardy, G.H. and Wright, E.M. (1960) The Theory of Numbers, Fourth Edition, Oxford University Press.
- Niven, I. and Zuckerman, H. (1960) An Introduction to the Theory of Numbers, Wiley

Some on line resources are:

- Elementary Number Theory Notes by W.W. Chen. See
<http://rutherglen.ics.mq.edu.au/wchen/lnentfolder/lnent.html>
- Elementary Number Theory on line book: Peter Hackman, 2009.
<http://www.mai.liu.se/~pehac/kurser/TATM54/booktot.pdf>
- Lecture notes on elementary number theory, by Bruce Ikenaga
<http://marauder.millersville.edu/~bikenaga/numbertheory/numbertheorynotes.html>
- Elementary Number Theory Notes, by William Stein, 2001
<http://modular.math.washington.edu/edu/Fall2001/124/>
- Number Theory Web
<http://www.numbertheory.org/ntw/>

Some famous number theorists:

- Johann Carl Friedrich Gauss. 1777-1855.
<http://www-groups.dcs.st-and.ac.uk/~history/Mathematicians/Gauss.html>
- Pierre de Fermat. 1601 - 1665.
<http://www-groups.dcs.st-and.ac.uk/~history/Mathematicians/Fermat.html>
- Leonhard Euler. 1707-1783.
<http://www-groups.dcs.st-and.ac.uk/~history/Mathematicians/Euler.html>
- Srinivasa Aiyangar Ramanujan. 1887-1920.
<http://www-history.mcs.st-andrews.ac.uk/Biographies/Ramanujan.html>
- Andrew John Wiles. 1953-
<http://www-groups.dcs.st-and.ac.uk/~history/Mathematicians/Wiles.html>