

Newer Math

Notes for the New Jersey Governor's School of Engineering and Technology of lectures given at the School of Engineering, Rutgers University, Piscataway, New Jersey in July 2004

by Stephen J. Greenfield
Department of Mathematics, Rutgers University
E-mail greenfie@math.rutgers.edu
Homepage <http://www.math.rutgers.edu/~greenfie>

Words of wisdom

Beauty is the first test: there is no permanent place in this world for ugly mathematics

G. H. Hardy (1877-1947)

Mathematics is an interesting intellectual sport but it should not be allowed to stand in the way of obtaining sensible information about physical processes.

Richard W. Hamming (1915-1998)

Introduction

The prerequisites needed for reading this material are “just” some high school algebra and knowledge of simple analytic geometry. And intelligence and concentration. Some sources of what’s here are hundreds of years old, but all the topics investigated are objects of current research, and are of fundamental importance to current applications. These topics are usually addressed in advanced undergraduate or graduate courses. Although the methods are elementary, the results are amazing and sometimes nearly unbelievable. There are many possibilities for students to contribute to these areas, but be aware that many smart and hardworking people are working on this material. I will mention some work which has been done within the last year! College courses discussing the ideas that follow may be given in Mathematics or Computer Science or Electrical/Comp[uter Engineering Departments, and may be entitled Cryptography or Number Theory or Probability or Networks or Combinatorics or Coding Theory or Algorithms ... but I won’t feel strictly bound by the names of subjects: I’ll try to tell you about interesting ideas and how these ideas are used. I’ll touch on some of the social questions involved. There certainly won’t be complete discussions about any of these subjects. I’ll try to present some good stuff. I will give further references, both to traditional sources such as books and to “new media” such as web links. Please report any needed corrections and do suggest improvements, which will be acknowledged.

Although I hope prerequisites for understanding this material are minimal, a quote on “high school” algebra from Carl Jung’s *Memories, Dreams, Reflections** may be interesting.

... All my life it remained a puzzle to me why it was that I never managed to get my bearings in mathematics when there was no doubt whatever that I could calculate properly. Least of all did I understand my own moral doubts concerning mathematics.

Equations I could comprehend only by inserting specific numerical values in place of the letters and verifying the meaning of the operation by actual calculation. As we went on in mathematics I was able to get along, more or less, by copying out algebraic formulas whose meaning I did not understand, and by memorizing where a particular combination of letters had stood on the blackboard. I could no longer make headway by substituting numbers, for from time to time the teacher would say, “Here we put the expression so-and-so,” and then he would scribble a few letters on the blackboard. I had no idea where he got them and why he did it—the only reason I could see was that it enabled him to bring the procedure to what he felt was a satisfactory conclusion. I was so intimidated by my incomprehension that I did not dare to ask any questions.

Mathematics classes became sheer terror and torture to me. ...

* Carl Jung (1875-1961) was a founder of modern psychiatry. For more information see <http://www.ship.edu/~cgboeree/jung.html>.

Contents

Lecture and title	Pages
Introduction	ii
#0: People and secrets	1-2
#1: Secret sharing	3-6
#2: Modular arithmetic	7-10
#3: Fermat and Euler	11-14
#4: Public key encryption	15-19
#5: How hard is arithmetic?	20-27
#6: Who owns ideas?	28-32
#7: More encryption	23-35
#8: Perfect cryptography	36-37
#9: Probably ...	38-40
#10: Gambling	41-45
#11: The transmission network	46-47
#12: Broadcasting – statement and heuristics	48-50
#13: Broadcasting – problem analysis	51-52
#14: Broadcasting – solution and discussion	53-55
#14 ^{1/2} : Intermezzo BIRTHDAY TIME!	56
#15: Pigeons and patterns	57-58
#16: Friends, strangers, and coloring graphs	59-63
#17: Ramsey and five	64-67
#18: Random graphs and real networks	68-69
#19: Coding theory	70

A collection of relevant links will be maintained on the homepage of these notes: look for **LINKS**

I hope this will help interested readers learn more.

The last two lectures are just placeholders with some references and a small amount of discussion. I don't think I'll get to these topics in the 14 sessions scheduled.