Codes

F10PC1 Pure Maths C
and
F11PE1 Pure Maths E

This is the first year this course has been taught and so there are no past exam papers. I shall provide you with a specimen exam paper towards the end of the semester.

Prerequisites

You need to be confident in manipulating matrices and calculating determinants; you need to be able to solve linear equations using Gaussian elimination; you need to understand the notions of linear dependence and independence. You need to have met the notions of group, ring and field before and have a general idea of what they mean; the one theorem from group theory we shall need is Lagrange's theorem which I shall quickly revise in the lectures. However, the most important prerequisite is that you enjoy algebra and would like to learn how algebraic ideas can be applied to problems in the real world.

Recommended books

The book by Biggs [2] covers the same topics as me although I shall omit much of the material he discusses on probability theory and instead I shall develop the algebraic side of the theory in more depth. I shall cover the following chapters:

- Introduction: Chapter 1.
- Cryptography: Chapters 10, 11, 12, 13.
- Error-correcting codes: Chapters 6, 8 and 9.
- Variable-length codes: Chapters 2 and 3.

The book by Childs [5] will be an extremely useful reference for the algebra. Both books are published by Springer and so can currently be downloaded for free.

Exams

- C-students will sit a 2 hour exam. This will consist of 4 questions and you will need to answer 3.
- E-students will sit a 3 hour exam. This will consist of 5 questions: 4 questions as above and one extra that will test the independent reading you will be asked to do. You will need to answer all questions.

Syllabus

(1) **Introduction** What this course is about: the mathematics of cryptography, error-correcting codes and variable-length codes and the roles they play in our lives. I shall give the formal definition in this section of what we mean by the word *code* in mathematics using the idea of a free monoid.

(2) **Cryptography** [21 lectures approximately]

(a) **Algorithms and complexity** An informal description of what algorithms are and why they are important; a description of what is meant by the time complexity of an algorithm, polynomial-time algorithms: tractable and intractable problems, the class **P**. An informal description of the question 'Is **P** equal to **NP**?' using the travelling salesman problem. Deciding whether a number is prime by trial division; the AKS-primality test (discussion but no details); deciding primality is in **P**.

(b) **Basic number theory** Gcd's, Euclid's algorithm, Euclid's *Elements*, Bézout's theorem, Blankinship's algorithm, Gauss's lemma, linear Diophantine equations; Fibonacci numbers and their properties, Binet's formula, estimates, Lamé's theorem. Primes, the fundamental theorem of arithmetic, the Fermat method for factoring numbers, the Sieve of Eratosthenes, the distribution of primes, the Prime Number Theorem (proof omitted). Binomial numbers: Mersenne numbers and perfect numbers; Fermat numbers and constructible polygons. Primes that can be written as sums of squares.

(c) **Basic algebra** Equivalence relations and partitions, modular arithmetic, exponentiation by repeated squaring. Semigroups, monoids, groups, abelian groups, rings, fields; direct products of rings, the Chinese remainder theorem. Euler's ϕ-function and its properties: arithmetic functions and multiplicative functions. Groups of units, cyclic groups; the structure of the group $\mathbb{U}_n$: it is cyclic if and only if $n = 1, 2, 4, p^2, 2p^e$ where p is an odd prime (no proof); Lagrange's theorem, the theorems of Euler, Fermat and Wilson; the primitive element theorem for $\mathbb{U}_p$ where p is a prime.

(d) **Symmetric and asymmetric codes** The basic questions of cryptology, cryptosystems and their history; Caesar ciphers, Vigenère ciphers, Hill ciphers; one-time pads; DES and AES; the difference between symmetric and asymmetric (public-key) cryptosystems: Diffie-Hellman key exchange; RSA codes.

(3) **Error-correcting codes** [9 lectures approximately]

(a) **Basic definitions and examples** The basic problem of noisy channels, redundancy, codes and codewords, nearest neighbour decoding principle, Hamming distance, minimum distance of a code, the Hamming bound, perfect codes, equivalence of codes.

(b) **Linear codes** Vector spaces over finite fields, generator and parity-check matrices, dual codes, syndrome decoding, equivalence of linear codes, Hamming codes: single-error correcting codes; multiple-error correcting codes: some simple examples.

The following topic will be studied by E-students only by reading the relevant chapters of Biggs.

(4) **Variable-length codes** Definition of a variable-length code, tree representation, the Kraft-McMillan number, prefix codes, entropy of a memoryless source, optimal codes, Huffman codes.

I have listed my main sources below. Note that the books by Devlin [7], Levy [17] and Singh [23] are highly recommended reading books.

References

[1] J. Baylis, *Error-correcting codes*, Chapman and hall, 1998.

[2] N. L. Biggs, *Codes*, Springer, 2008.

[3] C. B. Boyer, U. C. Merzbach, *A history of mathematics*, John Wiley and Sons, Second Edition, 1989.

[4] J. A. Buchmann, *Introduction to cryptography*, Second Edition, 2001.

[5] L. N. Childs, *A concrete introduction to higher algebra*, Second Edition, Springer, 2000.

[6] A. Clark, *Elements of abstract algebra*, Dover, 1984.

[7] K. Devlin, *The millennium problems*, Granta Books, London, 2002.

[8] W. Diffie, M. E. Hellman, New directions in cryptography, *IEEE Transactions on Information Theory* **22** (1976), 644–654.

[9] M. R. Garey, D. S. Johnson, *Computers and intractability*, W. H. Freeman and Company, New York, 1997.

[10] A. Granville, It is easy to determine whether a given integer is a prime, *Bulletin of the American Mathematical Society* **42** (2004), 3–38.

[11] G. H. Hardy, *A mathematician's apology*, CUP, 1992.

[12] R. Hartshorne, *Geometry: Euclid and beyond*, Springer, 2000.

[13] R. Hill, *A first course in coding theory*, Clarendon Press, Oxford, 1986.

[14] G. A. Jones, J. M. Jones, *Elementary number theory*, Springer, 1998.

[15] N. Koblitz, *A course in number theory and cryptography*, Springer, 1994.

[16] W. J. LeVeque, *Fundamentals of number theory*, Dover, 1977.

[17] S. Levy, *Crypto*, Penguin, 2002.

[18] O. Ore, *Number theory and its history*, Dover, 1948.

[19] N. R. Reilly, *Introduction to applied algebraic systems*, OUP, 2010.

[20] R. L. Rivest, A. Shamir, L. M. Adleman, A method for obtaining digital signatures and public-key cryptosystems, *Communications of the ACM* **21** (1978), 120–126.

[21] B. Schneier, *Applied cryptography*, Second Edition, John Wiley and Sons, 1996.

[22] L. E. Sigler, *Fibonacci's Liber Abaci*, Springer, 2003, page 404.

[23] S. Singh, *The code book*, Fourth Estate, 2002.

[24] I. Stewart, *Galois theory*, Second Edition, Chapman and Hall, 1998.

[25] W. Stallings, *Cryptography and network security*, Third Edition, Prentice Hall, 2003.

[26] J. Stillwell, *Elements of algebra*, Springer, 1996.