COMP26120: Algorithms and Imperative Programming
Lecture 9: How to Pass the January Examination

Ian Pratt-Hartmann

Room KB2.38: email: ipratt@cs.man.ac.uk

2017–18
• Basic complexity measures
  • big-$O$ notation
  • big-$\Omega$-notation
  • simple examples of computing upper complexity bounds.

• Euclid’s algorithm
  • correctness
  • complexity

• Modular arithmetic
  • primitive roots
  • fast modular exponentiation
  • discrete logarithms
  • the El Gamal public key cryptosystem
• **Sorting**
  - Quicksort, bubblesort, mergesort, bucketsort . . .
  - Complexity and correctness
  - Lower bound on comparison-based sorting algorithms

• **Determinants and permanents**
  - Definitions
  - Permutations and parity
  - Computing determinants in cubic time
- **Reading:**
  
  http://studentnet.cs.manchester.ac.uk/ugt/2017/COMP26120/syllabus/

- **Past exam papers:**
  

Note that the syllabus may vary slightly from year to year.