

Review Topics Exam 2 18.310 2002

1. Euclid's Algorithm perform it to find gcd and express same as linear combination of original numbers with integer coefficients
2. The Chinese remainder theorem use it to prove statements about solutions to equations mod products of primes
3. Groups and Lagrange's theorem: be prepared to prove it and use it
4. symmetries of the square and multiplication table of them what are they?
5. FFT set up an $N=16$ fft and use it to multiply 2 8 digit numbers
6. RSA create an rsa code and code and decode with it
7. raising to a power mod n : be prepared to do it
8. finding primes" explain how it is done: find one in a certain range with a spreadsheet
9. testing primality describe and apply test
10. linear programming: model a situation, esp network flow or resource allocation
11. the quadratic sieve describe it
12. the tortoise and the hare be prepared to do it on a spreadsheet
13. magic determinant finding; set up spreadsheet and do this
14. doing the simplex algorithm be able to do pivots on a spreadsheet
15. finding a feasible origin explain how this is done
16. duality take the dual of a given primal; (doing this right requires practice!)
17. multiplying matrices set up a spreadsheet to do this
18. graphs and planarity outline proof of Kuratowski's theorem
19. five color theorem prove it
20. eulers formula state and prove it

be prepared to set up spreadsheets to implement

1,5,6,7,8,9,12, 13,14,17

be cognizant of the meaning of

2 3 4 10 11 15 16 18 19 20