

Exam #1 Study Questions -

1. Finding Primes — Describe a reasonably efficient way to find 100 decimal digit primes.
2. Raising to a power — Describe an efficient way to raise a number, x , to a high power, y , mod a large number, z .
3. Groups and Lagrange's theorem: — be prepared to state it, prove it, and use it.
4. Euclid's algorithm — Given 10 digit integers, A and b , how would you implement finding their gcd on a spreadsheet? Expressing that gcd as a linear combination of A and B ?
5. Chinese Remainder Theorem — State and prove this theorem.
6. Chinese Remainder Theorem — Explain how would you find a number mod PQ that was congruent to A mod P and B mod Q , where P and Q are two relatively prime large numbers.
7. RSA Algorithm — Explain how it works.
8. Carmichael Numbers — Define Carmichael numbers. Prove that a product of two primes PQ cannot be a Carmichael number.
9. Five color theorem — State and prove it.
10. Kuratowski Theorem — Which of the following graphs are planar (where the graph is described by edges as vertex pairs or as a diagram).
11. Describe how one multiplies numbers using the FFT.
12. FFT — Implement it on a spreadsheet using 32^{nd} roots of unity.
13. What is the basic recursion of the FFT?
14. What is the Finite Fourier Transform and how can it be inverted?
15. Explain the optimal strategy for finding the best rank in sequential choice. Prove that it is optimal. How well does it work?
16. Sequential Choice — Use a spreadsheet to compute the exact probability of successfully choosing the best choice in a sequential situation with 20 candidates. Where is the best threshold?
17. Sequential Choice — Use a spreadsheet to find the best strategy for minimizing the expected rank in a sequential situation with 20 candidates.
18. Generating Functions — Find the formula for the number of ways of tiling a $2 \times n$ strip with 2×1 tiles.
19. Generating Functions — Find the formula for the number of ways of tiling a $3 \times n$ strip with 2×2 and 1×1 square tiles.
20. Counting Trees — Let $d(i,T)$ be the degree of vertex i in tree T . If you sum

$$x_1^{d(1,T)-1} x_2^{d(2,T)-1} x_3^{d(3,T)-1} \dots x_n^{d(n,T)-1}$$

over all labeled trees T with n nodes, you obtain

$$(x_1 + x_2 + \dots + x_n)^{n-2}.$$

Use this formula to calculate the number of trees where the degree of vertex 1 is exactly k .