

Final Exam Study Guide**The Final Exam is Monday, May 5, 1:45 to 3:45 in Earth Sciences 101**

1. Approximately $2/3$ of the final exam will cover chapters 16, 17, 18, 19, 20, and 22, i.e., the material since the second hour exam. For this material you should make sure that you can do RSA problems as Alice (encrypter), Bob (decrypter), and Eve (enemy spy). You should also make sure that you can use Fermat's theorem and Euler's theorem to compute powers and roots in modular arithmetic (chapters 18, 19, 20), and make sure you can compute fractions in modular arithmetic (chapter 17). If there are 15 problems on the final exam, about 10 of these problems will cover material since the second exam.
2. **PRACTICE FINAL:** See the course website for practice finals:
 - (1) Practice final without answers: www.nd.edu/~sevens/practicefinal.pdf
 - (2) Practice final with answers: www.nd.edu/~sevens/practicefinan.pdf
3. For earlier material, I would start with the exams, and make sure you can do problems like the exam problems. Ask for help if there is a problem from Exam I or Exam II that you have trouble doing. Practice problems for Exams I and II are on the course website. I would also recommend going over quizzes in the same way. I would expect that problems covering chapter 15 and earlier on the final will be fairly similar to problems from Exam I or II, or from the quizzes.
4. Part I
Topics: Expect 1 or 2 problems here
 - Basic counting (ch. 1)
 - multiplication and subtraction principles (ch. 2, 3)
 - counting collections (ch. 4)
 - pascal's triangle and binomial coefficients (ch. 6)
5. Part II
Topics: Expect 3 or 4 problems here
 - Divisibility of integers, lcm, gcd, Euclidean Algorithm (ch. 8)
 - Combinations (when can you write 1 as a combination of \mathbf{a} and \mathbf{b} ?), the "backwards" Euclidean Algorithm ¹. (ch. 9)
 - Prime numbers, prime factorization, Sieve of Eratosthenes (ch. 10)

¹Be sure that you can carry out this algorithm when asked to solve equations like $1 = X \cdot a + Y \cdot b$ for X and Y

- Two definitions of prime number (one from ch. 10, the other from ch. 11), divisibility of binomial coefficients by primes, uniqueness of prime factorization (ch. 11)
- Consequences of prime factorization, e.g. how to compute **lcm** and **gcd** using factorizations, divisibility of fractions and binomial coefficients ² (ch. 12)
- Definition of two numbers being relatively prime, Euler ϕ function and how to compute it using the formula (ch. 13)

6. Part III

Topics: Expect about 10 problems here

- Basic modular arithmetic (how to add, subtract, multiply), abstract definition of fractions, reciprocals, roots (ch. 15)
- Congruence (how to tell if two numbers are congruent $(\text{mod } n)$), simple tricks for computing things $(\text{mod } n)$ (section 16.4) (ch. 16)
- Division, existence of fractions and reciprocals $(\text{mod } n)$ when n is prime and when it's not. You should be able to compute the reciprocal of a number $(\text{mod } n)$ using the techniques from Ch. 9 (backwards E.A.) (ch. 17)
- Powers, how to compute powers using the "method of squaring" (section 18.2), Fermat's Theorem and how to use it when computing powers, reciprocals, and roots $(\text{mod } n)$ when n is prime). (ch. 18)
- Roots $(\text{mod } n)$ when n is prime. In particular how to compute them, and when do they exist. (ch. 19)
- Euler's Theorem and how to use it when computing powers, reciprocals, and roots $(\text{mod } n)$ when n is **not prime** ³. Be sure you know when Euler's Theorem applies and when it doesn't (there are things you need to check before you use it) (ch. 20)

7. Part IV

Topics:

- How the RSA code works and how to implement it ⁴ (i.e. to encode or decode a message when the numbers involved are small enough to work by hand) (ch. 22)

²this concept seemed to be difficult for most people

³Remember that Fermat's Theorem is just a special case of Euler's Theorem. Euler applies no matter whether n is prime or not.

⁴It's good to remember what I called the various numbers involved. In particular remember what role n plays vs. what k is; also p , q , a , and b . Try not to mix up n (the modulus) and k (the power), or a (the original message) and b (the encoded message).

- THE END. Good luck on the exam, and have a great summer.

Practice problems for Ch. 17 - Ch. 20

1. (Ch. 17) 17.3.2, 17.3.3
2. (Ch. 18) HW #9 problems: 18.2.1, 18.6.3, 18.6.4
3. (Ch. 19) HW #9 problems 19.2.1, review example 19.4.1 (page 212), exercise 19.4.2
4. (Ch. 20) Review example 20.4.1 (page 224) and example 20.4.2, do exercise 20.4.3
5. Use Euler's Theorem to answer the following questions:
 - (a) What is $7^{1337} \pmod{18}$? (Answer: **13**)
 - (b) Does $\sqrt[11]{5} \pmod{18}$ exist? If so, compute it. (Answer: **11**)
 - (c) How many numbers $X \pmod{18}$ satisfy the equation: $X^{12} \equiv 1 \pmod{18}$? (Answer: **18**)

Note: The problems above which do not have an answer attached have solutions on the course web page under the "solutions" category.

Practice problems for Ch. 21 - Ch. 24

1. (Ch. 22) Exercise 22.3.1 (Answer: **196**)
2. (Ch. 22) Quiz #6 problems (Answers: $16 \pmod{21}$ for (a), $20 \pmod{91}$ for (b)).
3. (Ch. 22) Alice wants to send a secret message to Bob using public-key cryptography. Upon request, Bob sends her $n = 143$ and $k = 17$. If Alice wants to tell Bob that **2** people are coming to dinner, but she wants to encrypt the message, what should she send Bob? (Answer: **84**)