Final Exam Study Guide

Theory of Numbers (Fall 2014)
Rutgers University
Swastik Kopparty

Concepts and theorems

1. Proofs by induction, strong induction
2. Primes, unique factorization, infinitude
3. GCD, Euclid's algorithm, Bezout's lemma
4. Base q representations
5. the number of divisors of a number, the sum of divisors of a number, Euler's totient function
6. congruences mod m
7. $\mathbb{Z}_m$ and $\mathbb{Z}_m^*$. The different definitions of $\mathbb{Z}_m^*$, and their equivalence.
8. The Chinese remainder theorem
9. order of an element of $\mathbb{Z}_m^*$, Fermat's little theorem, Euler's theorem
10. the math behind the RSA cryptosystem (basically covered by the above)
11. quadratic residues mod a prime, their number, closure under multiplication
12. the quadratic residue symbol, how to compute it
13. Pythogorean triples
14. prime factorization of $n!$
15. the number of primes less than n
16. linear recurrences, Fibonacci numbers
17. the Riemann zeta function, factorization, Euler's proof of infinitude of primes
18. partitions of an integer, generating function for partitions
19. Gaussian integers, application to expressing primes as a sum of two squares
20. divisibility tests, even for numbers written in a different base
21. decimal expansions of rational numbers

Numerical problems

Here are some samples of the kinds of numerical problems that you should be able to solve (this is by no means a complete list). Some problems are harder than others.

1. Show by induction on n that $F_n \leq 2^n$ for all $n \geq 0$ (where F_n is the n'th Fibonacci number).
2. Define a sequence A_n as follows: $A_0 = 1$, and for each $n \geq 1$, $A_n = 1 + \sum_{j=0}^{n-1} A_j$.

   Prove that $A_n = 2^n$ for all $n \geq 0$.
3. Write $(4123)_5$ in base 10. Then write it in base 3 and base 16.
4. Find the GCD of 9711 and 816. Express this GCD as an integer combination of 9711 and 816.
5. Find an integer a such that $a \cdot 816 \equiv 1 \mod 9713$.
6. Find an integer b such that $b \cdot 815 \equiv 75 \mod 9713$.
7. Show that there is no integer a such that $a \cdot 21 \equiv 11 \mod 15$.
8. Compute the remainder when 17^{86} is divided by 23.
9. Describe the set of all $n \in \mathbb{Z}$ which satisfy $n^3 + 1 \equiv 0 \mod 11$.
10. Find an integer e such that $7e \equiv 1 \mod 190$. Show that for this integer e, we have that for every $a \in \mathbb{Z}_{191}^*$, $a^{7e} \equiv a \mod 191$.

    Based on what you did above, how would you find an integer e such that for every $a \in \mathbb{Z}_{166}^*$, $a^{11e} \equiv a \mod 166$.
11. Let S be the set of integers x satisfying both the following equations:
    - $x \equiv 7 \mod 133$,
    - $x \equiv 11 \mod 29$.

    Find S. Express your answer as " $S = \{n \mid n \equiv a \mod b\}$" for some integers a,b.

    For example, if the problem was:
    - Let S be the set of integers x satisfying both the following equations:
      - $x \equiv 2 \mod 4$,
      - $x \equiv 3 \mod 7$.

      Find S.

    Then the answer is "$S = \{n \mid n \equiv 10 \mod 28\}$".
12. Let S be the set of integers x satisfying both the following equations:
    - $2x \equiv 1 \mod 13$,
    - $3x \equiv 1 \mod 17$.

Find S. Express your answer as " $S = \{n \mid n \equiv a \mod b\}$" for some integers a,b.

13. Is 89 a quadratic residue mod 31? Is 89 a quadratic residue mod 101? Is 89 a quadratic residue mod 111?

    (101 is a prime, 111 is not).

14. Suppose $x^2 - y^2$ is prime. Show that $2y + 1$ is prime.

15. Show that 13 is not a prime in the Gaussian integers by exhibiting a factorization of 13.

16. List all the partitions of 5.

17. True or false: let $p_1, .., p_t$ be the first t primes. Then $p_1 \cdot p_2 \cdot \ldots \cdot p_t + 1$ is a prime.

18. Let p be a prime, and let $a, b \in \mathbb{Z}_p^*$.

    Show that if a is a quadratic nonresidue mod p, and b is a quadratic nonresidue mod p, then $a \cdot b$ is a quadratic residue mod p.

19. What is the largest power of 3 that divides 40!.

20. Show that for all n, the number $n \cdot (n + 7) \cdot (n + 26) \cdot (n + 325)$ is divisible by 24.

21. Give a divisibility test for to test if a given number is divisible by 35. The test should be in terms of the digits of the number when written in base 6.

    Give your answer in the form: "The number $a = (a_k a_{k-1} \ldots a_0)_6$ is divisible by 35 if and only if (something involving the digits...) ".

    Is $(143125)_6$ divisible by 35?

22. What are the possible values of $n^4 \mod 13$ where n is an integer.

    Use this to show that there are no integers x, y such that $x^4 + y^4 = 39000005$.

23. What are the possible values of $n^{100} \mod 101$, where n is an integer.

    Use this to show that there are no integers x, y, z, a such that $x^{100} + y^{100} + z^{100} = 101a + 7$.

24. Find the sum of divisors of 100. Find the total number of divisors of 100. Find $\phi(100)$.

25. True or false: If $a \equiv b \mod c$, then $2^a \equiv 2^b \mod c$.

26. Give an example of an integer n such that 2 and 3 are both in $\mathbb{Z}_n^*$, and $\text{ord}_n(2) < \text{ord}_n(3)$.

    Give an example of an integer n such that 2 and 3 are both in $\mathbb{Z}_n^*$, and $\text{ord}_n(2) > \text{ord}_n(3)$.

27. Show that for every integer n such that 2 and 4 are both in $\mathbb{Z}_n^*$, we have $\text{ord}_n(2) \leq \text{ord}_n(4)$.

Other problems

There will also be a few problems where you would have to prove some statements, using your understanding of the concepts and theorems. These problems will be easier than your homework problems and quiz problems.