Practice Questions for the Final Exam

The following consists of practice questions to help you prepare for the final. They are similar in style and difficulty (although some of these may be a bit harder) to what will be on the final, although also more numerous (the final will consist of ten questions). We won't be collecting or grading them, but we encourage you to work through them. We will be posting solutions sometime next week.

1. Ian and Nai play the game of todo, where at each stage one of them flips a coin and then rolls a die. The person who played gets as many points as the number rolled plus one if the coin came up heads, and the number rolled minus one if the coin came up tails. For example, if Ian gets heads and rolls a 3, he gets 4 points, whereas if Nai gets tails and rolls a 6, he gets 5 points.

   (a) What is the probability that a person gets 7 points in one turn?

   (b) Ian just made 3 points. What is the probability that Nai will get more points in his turn?

   (c) In the above situation, what is the probability that Nai will get the same number of points?

2. Four standard 6-sided dice are rolled.

   (a) What is the probability that the sum of the values shown is 5?

   (b) What is the probability that all four dice show different values?

   (c) What is the probability that only 1's, 2's and 3's occur but not all dice show the same value? (Note that not all three numbers have to occur, e.g. 2223 is a valid outcome.)

3. Prof. Elkies is making bracelets for his nieces. Each bracelet has 23 beads, and each bead may be any of the three colors blue, pink, and purple.

   (a) How many possible bracelets are there?

   (b) Of those, how many use at least two different-colored beads?

   (c) One niece asks that her bracelet include at least one bead of each of the three available colors. How many such bracelets are there?

   (d) Another niece insists that more than half of her beads be purple, her favorite color. How many such bracelets are there?

   Remark: Since 23 is prime, you can check that your answer to the second part must be a multiple of 23. Can you see this directly? (One can give yet another proof of Fermat's theorem this way.)

4. You are playing Scrabble$^{\text{TM}}$, and draw the letters EEESSTT.

   (a) In how many ways can you arrange these letters to form a 7-letter "word"?

   (b) If you choose one of these arrangements randomly, what is the probability that you will make one of the two actual words SETTEES and TESTEES that these letters form?

   (c) If you choose one of the arrangements of your letters EEESSTT randomly, what is the probability of getting the three E's in a row (as in EEESSTT or SEEETTS, but not ESESETT or TSETSEE)?

5. Suppose a kindergarten class has 7 girls and 3 boys.

   (a) How many ways are there to put the students in a line if we require that the first and last people in line are both girls?

   (b) Suppose that the class must be divided into two groups, with 5 of them going outside to recess and the other 5 staying inside to study math. How many ways are there to do this?

   (c) Suppose that each of the two groups from the previous part must contain students of each gender. Now how many ways are there of putting the students into groups?

6. Florian picks three cards at random out of a 52 card deck, records them, and returns them to the deck. Grigor does the same (he picks three cards at random out of the 52 card deck, and records them).

   (a) What is the probability that at least one card will have been chosen by both Florian and Grigor?

   (b) What is the probability that none of Florian's cards are aces?

7. (a) Are there solutions to the equation

   $$22 = 23X + 21Y$$

   in whole numbers (X, Y)? If so, find *two* solutions (X, Y).

   (b) What is the least common multiple of 96 and 162?

8. Let $c = \binom{24}{11}$.

   (a) Is c divisible by 17?

   (b) Is c divisible by 15?

   (c) For what numbers m does the equation $c \cdot x + 29y = m$ have a solution (where, as usual, we mean a solution with x and y being whole numbers)?

9. (a) Which is bigger, 22^5 or $\binom{22}{17}$?

   (b) Is $\binom{22}{17}$ even or odd?

   (c) Which prime numbers p bigger than 11 are divisors of the number $\binom{22}{17}$?

10. In the first two parts of the following problems please write the answer as product of powers of prime numbers.

    (a) Find the least common multiple A of the numbers from 1 to 10 (inclusive).

    (b) Compute $\phi(10!)$.

    (c) How many numbers divide $\phi(10!)$ but not A?

11. (a) Given that 2 is a generator for arithmetic modulo the prime 53, how many square roots does 2 have modulo 53?

    (b) How many square roots does 1 have modulo 51? Find them all.

(c) How many square roots does 0 have modulo 49? Find them all.

12. (a) Find all odd numbers n such that $\phi(n) = 6$. (**Hint:** Use Euler's theorem.)
    (b) Find all numbers n such that $\phi(n) = 6$.
    (c) For each of the composite numbers n such that $\phi(n) = 6$, find a witness for the fact that they are not prime.

13. (a) Find a generator G for arithmetic modulo the prime 23. Make a table of x and G^x for each $x = 0, 1, 2, \dots, 21$.
    (b) Use your table to quickly compute each of the following mod 23:
        i. 11×13
        ii. $11/13$
        iii. 11^{13}
        iv. G^{219}
    (c) Use your table to find a square root of 6 mod 23. Check your work by verifying directly that it is in fact a square root.

14. Let p be one of the primes $3, 5, 7, 11, 13$.
    (a) For which p does 2 have a square root $\pmod p$?
    (b) For each one for the possibilities for p find a generator $\pmod p$.

15. Suppose we are given that 3 is generator $\pmod{17}$.
    (a) How many numbers $\pmod{17}$ have a cube root $\pmod{17}$?
    (b) Find all solutions to $x^3 \equiv 3 \pmod{17}$.
    (c) Find all pairs x, y of integers $\pmod{17}$, where neither one is allowed to be zero, such that $x^4 + y^4 \equiv -1 \pmod{17}$

16. Express the answer to these numerical questions mod 23 in terms of the congruence classes

$$\{0, 1, 2, 3, \dots, 22\}.$$

    (a) $22^3 \pmod{23}$
    (b) $3^{22} \pmod{23}$
    (c) $3^{33} \pmod{23}$ (Hint: $3^3 \equiv 2^2 \pmod{23}$.)

17. Alice and Bob must communicate via an insecure channel, but have no real reason to keep anything that say private. Nevertheless, veterans of QR28 that they are, Bob proposes that they practice the public key code method taught in QR28, but for a choice of ridiculously small (odd) prime numbers P and Q. That is, Bob will choose two primes P and Q and form the product $N = P \cdot Q$. He will then choose a number k *for which the code will actually work,* and will send to Alice the numbers N and k. As usual, he will then ask Alice to encode her message as a number a and "publish" (that is, send back to him via the insecure channel) the quantity a^k modulo N. For some curious reason, Bob is bent on choosing $k = 15$. What are the smallest distinct prime numbers P and Q that he can use to manufacture the $N = P \cdot Q$ he will be sending to Alice?

18. Alice and Bob wish to exchange messages using the RSA encryption scheme. First, Bob chooses $p = 11$ and $q = 19$ as his secret, "large" primes. He publishes their product, $N = 209$, and he also chooses and publishes $k = 23$ as the encryption exponent.

    (a) If Alice wishes to send the message 35 to Bob, what should she send?

    (b) If Bob receives the transmission 5, what was Alice's message?

19. Alice and Bob wish to use the password scheme we've discussed. They choose 23 as their prime and 7 as a generator for arithmetic (mod 23). Alice chooses 5 as her secret exponent, and then she publishes 17. Bob chooses 8 as his secret exponent and publishes 12. What is their password?

20. Compute $9^{\left(4^{163}\right)} \pmod{99}$.

21. A number x between 1 and 30, inclusive, is chosen at random.

    (a) What is the probability that x is a generator in arithmetic modulo 31?

    (b) What is the probability that x has a fourth root modulo 31?

    (c) What is the probability that x is a square but not a cube modulo 31?

22. (a) Find generators modulo each of the following prime numbers: 5, 7 and 11.

    (b) Using your answer to (a), or otherwise, find all the squares mod 11.