QR 28 - The Magic of Numbers
Practice Final

Friday December 19th, 2008

Time allowed: 180 minutes

- Calculators *will* be allowed, but no other notes, books or other study aids will be allowed.
- This practice final is divided into two parts. The first part consists of a series of questions of approximately the length of the real final. We advise that you attempt this part under test conditions, giving yourself three hours to complete it.

  The second part consists of extra problems, possibly covering material not included in the first part. You will are responsible for the ideas covered in these extra problems, as well as material on the homework and exams.
- In the first part, we have given point values to the different questions. To see how many points are awarded to parts (a), (b), (c) etc., look for numbers in parentheses in the right hand margin.

1 Timed Section

1. Every book is given a unique number called the International Standard Book Number (ISBN) that identifies it. The ISBN number is a 9 digit number. For example, the ISBN number of the course textbook is 013177721.

   (a) Suppose that any 9 digit number is allowed as an ISBN. How many different ISBN's are there? (2)

   (b) Suppose that we continue to assume that all 9 digit numbers are allowed as an ISBN. How many possible ISBN's contain no 4? (4)

   (c) Now suppose that the last digit of an ISBN number must be congruent to 1 modulo 2. For example, the number 013177721 is allowed since (4)

   $$1 \equiv 1 (\text{mod } 2).$$

   Now how many different ISBN's are there?

2. There is a revolution at Harvard and the student government is reorganized. Instead of a president, vice-president, and so forth, the student government is organized as follows. The head of student government will be known as the Chairman. In addition to the chairman, there are two different legislative bodies - the Congress of Student's Deputies, consisting of 23 students, and the Council of Students, consisting of 43 students. There are 6,715 undergraduates at Harvard.

   (a) How many ways are there to choose just members of the Council of Students from the student body? Assume that every student is eligible. (2)

   (b) Suppose that no student can occupy more than 1 position (e.g. no one can be both Chairman and a member of the Congress of Student's Deputies)? In how many different ways can the positions of Congress of Student's Deputies, Council of Students, and Chairman be filled? (4)

   (c) Now suppose that the Chairman is considered a member of both the Congress of Student's Deputies and a member of the Council of Students. Now how many different ways can the student government be formed? (4)

3. (a) You roll 3 standard dice. What's the probability that the sum of the faces is exactly equal to 3? (2)

(b) Suppose instead that you roll 2 standard dice. Now what's the probability that the sum of the faces is exactly equal to 3? (3)

(c) Now suppose that you roll 5 standard dice. What is the probability that they all show different numbers? (5)

4. Consider the word "FARAFANGANA," a city in southeastern Madagascar.

   (a) How many ways are there to rearrange its letters? (2)

   (b) How many of the rearrangements in part (4a) do not have the Fs next to one another? (4)

   (c) How many of the rearrangements in part (4a) have exactly 3 letters separating the two Fs, like in the original word? (4)

5. (a) Is there a number $n > 1$ for which $\phi(n) \geq n$? (2)

(b) Starting with $n = 100$, compute $\phi(n)$, and then ϕ of your answer, and then ϕ of that, and ϕ of that until you've computed ϕ six times. That is, compute $\phi(100)$, $\phi(\phi(100))$,..., $\phi(\phi(\phi(\phi(\phi(\phi(100))))))$. (2)

(c) Explain why, starting with any number n, if you compute $\phi(n)$, then $\phi(\phi(n))$, etc., you'll eventually reach 1. (2)

(d) Compute $98^{83^{17}}$ mod 100. (4)

6. Compute the following numbers modulo 51. Express your answer as a number x with $0 \leq x \leq 50$.

   (a) $1/20$ (2)

   (b) $5^{1/11}$ (3)

   (c) 6^{32} (3)

   (d) 50^{50} (2)

7. Which of the following equations have solutions x and y with x and y integers? You don't need to give a solution. Simply indicate the ones that do.

(a) 5 x - 72 y = 1 (2)

(b) 35 x + 49 = 21 (2)

(c) 34 x + 35 y = 17 (2)

(d) 2 x + 26 y = 7 (2)

(e) 2 x + 3 y = 0 (2)

8. One way that RSA is used in real life is as a digital signature. (**NB: this problem is about a new idea in cryptography, namely digital signatures. It only uses techniques that you've seen before, but you shouldn't feel bad if it takes you a little while to wrap your head around why this all works**) Suppose that Alice published her public keys $n = 9223$ and $k = 13$ years ago.

   (a) In order to decrypt messages, Alice raises it to a certain power d modulo n (we call this process "decrypting"). What is Alice's decryption exponent d? (2)

   (b) Alice wants to send the message 404 to Bob. She doesn't care if other people can read the message, but wants Bob to be certain that she wrote it. She can do this by *decrypting* 404 and sending both 404 and the decrypted version (the signature) to Bob. Bob can then encrypt the signature using Alice's key, and he'll know the message is from her and hasn't been tampered with if the encrypted signature matches the message. Why does this work? (4)

   (c) Suppose that Eve wants to send the message 1337 to Bob, posing as Alice. What should she send? (4)

9. (a) Determine if 512461 is prime or composite using the Miller-Rabin test. For the purpose of this problem, we shall call it "prime" if it passes the test for bases 2 and 3. (5)

(b) Determine if 512467 is prime or composite using the Miller-Rabin test. For the purpose of this problem, we shall call it "prime" if it passes the test for bases 2 and 3. (5)

10. Consider the following table of powers modulo 19.

x	x^2	x^3	x^4	x^5	x^6	x^7	x^8	x^9	x^{10}	x^{11}	x^{12}	x^{13}	x^{14}	x^{15}	x^{16}	x^{17}	x^{18}
2	4	8	16	13	7	14	9	18	17	15	11	3	6	12	5	10	1

(a) Is 2 a multiplicative generator modulo 19? (1)

(b) Does -1 have a square root modulo 19? If so, find all x such that $x^2 \equiv -1 \pmod{19}$. (2)

(c) How many generators are there modulo 19? (2)

(d) Write down all of the generators modulo 19. (2)

(e) Find all x such that $x^3 \equiv 1 \pmod{19}$. (2)

2 Extra Problems

11. (a) How many numbers are there between 17 and 289 inclusive?
    (b) How many of the numbers in part (a) are not divisible by 8?
    (c) How many of the numbers in part (a) are not divisible by 8 or 12?

12. Jesse is choosing courses for the 2008-2009 school year. There are 5 music courses, 7 history courses, 11 language courses and 14 math courses that he is interested in taking, all of them one semester courses, and all of them offered in both the fall and the spring.

    (a) He decides to take one of each kind of course in the fall semester. How many ways are there to choose his courses?

    (b) In the spring, he decides to take 2 math courses and 2 language courses. If he doesn't want to repeat any of the courses from the fall, how many choices are there?

    (c) Jesse later discovers that one of the math courses is a prerequisite for another. Given this new information, how many ways can Jesse choose all his courses for the year (distributed as in parts (a) and (b))? **Hint:** either he takes the prerequisite in the fall, or he doesn't; count these two cases separately.

13. Every year, the annual Pacific wine festival invites the 10 best domestic wineries to participate. In contention for the 2009 festival are 35 California wineries, 23 Oregon wineries and 19 Washington wineries.

    (a) In how many ways can the participants be chosen if there must be 4 from California, 3 from Oregon and 3 from Washington?

    (b) In how many ways can the participants be chosen if the only condition is that there be at least one Oregonian winery?

    (c) In how many ways can the participants be chosen if the only condition is that there be at most 2 Californian wineries?

    (d) In how many ways can the participants be chosen if each of the three states must send at least one representative?

14. Ian and Nai are playing the game todo, where on each turn 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 flips 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?

15. In a modified version of poker, called "Flusher," the only winning hand is a flush – 5 cards all of the same suit. Remember that a standard deck contains 52 cards, 13 in each of 4 different suits.

    (a) What is the probability of being dealt a winning hand in Flusher?

    (b) In Flusher, you actually get 2 tries at the flush: after being dealt the initial hand, you can give any number of cards back to the dealer. The dealer will put them back in the deck, shuffle it again, and give you enough cards to replace the ones you discarded. If you are dealt 4 hearts and 1 spade, and you discard the spade, what is the probability of winning?

    (c) If you are dealt 2 clubs, 1 diamond, 1 heart and 1 spade, is it smarter to keep the 2 clubs and draw 3 cards, or discard the whole hand and draw 5 cards?

16. Mr. Hopkins' kindergarten class contains 8 boys and 8 girls.

    (a) In how many ways can Mr. Hopkins line up the 16 children?

    (b) In how many ways can he line them up if no two boys are permitted to stand next to one another?

17. (a) Use the Euclidean Algorithm to find the greatest common divisor of 196 and 217.

    (b) Find whole numbers x and y such that $196x + 217y = 7$.

18. Which numbers between 280 and 300 are prime?

19. Let $m = 5130$ and $n = 5544$.

    (a) What is the greatest common divisor of m and n.

    (b) How many positive whole numbers divide m?

    (c) How many positive whole numbers divide either m or n? Note that this implicitly includes numbers that divide both.

20. Let $\phi(n)$ denote Euler's phi function. Compute:

    (a) $\phi(589)$;

    (b) $\phi(600)$;

    (c) $\phi(625)$;

    (d) $\phi(666)$.

21. Let $c = \frac{41!}{11! \cdot 13! \cdot 20!}$. It is a fact that c is a whole number.

    (a) Is c divisible by 29?

    (b) Is c divisible by 5?

    (c) Is c divisible by 25?

    (d) What is the largest number k such that c is divisible by 2^k?

22. Do the following calculations in the given modulus. Your answer should be a number in the range $\{0, 1, \ldots, m-1\}$, where m is the modulus.

(a) $6 \cdot 11 \pmod{31}$.

(b) $4 - 13 \pmod{28}$.

(c) $81 \cdot 82 \cdot 85 \pmod{83}$.

(d) $1000! \pmod{1001}$.

(e) $99^{100} \pmod{101}$.

(f) $1/3 \pmod{23}$.

(g) $1/16 \pmod{79}$.

23. Compute the following powers $\pmod{21}$. Your answer should be a whole number between 0 and 20.

    (a) $2^{80} \pmod{21}$

    (b) $3^{84} \pmod{21}$

    (c) $5^{97} \pmod{21}$

24. Compute the fifth root of $3 \pmod{29}$. Your answer should be a number between 0 and 28.

25. What are the last two digits of 23^{10201}?

26. Alice and Bob must communicate via an insecure channel, but have no real reason to keep anything they 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 send the number $a^k \pmod{N}$ back to him. 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?

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

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

28. **Try doing this problem without a calculator**

    (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 $\binom{22}{17}$?