Math 187 Test IV, Spring 2012

Dr. Holmes

April 26, 2012

The exam will begin at 140 pm and end at 235 pm. You may use your writing instrument, your non-graphing scientific calculator, and your test paper. If you require scratch paper I will have some.
1. Find a solution to the system of equations

\[ x \equiv 6 \mod 13 \]
\[ x \equiv 9 \mod 19 \]

Find another solution (hint: what is the appropriate modulus?)
2. Necklace counting

(a) A closed necklace with no clasp has 11 beads of 4 colors. How many such necklaces are possible?

(b) (extra credit) A closed necklace has 15 beads of 3 colors. How many such necklaces are possible?
3. Modular exponentiation

(a) Compute $7^{435627650} \mod 13$ Hint: Fermat’s little theorem makes this a snap.

(b) Compute $11^{1024} \mod 100$ (a different set of tricks makes this straightforward)
4. Degree sequences

(a) For each of the two following degree sequences, either draw a graph with that degree sequence or give a brief explanation as to why there cannot be one.

i. 4, 4, 3, 2, 2, 1

ii. 4, 3, 3, 2, 2, 1

(b) Show me two nonisomorphic graphs with the degree sequence 2, 2, 2, 2, 2
5. One of the two pictured graphs has an Eulerian trail. One doesn’t. Explain why the one that doesn’t, doesn’t, and give an Eulerian trail for the other in the form of a list of vertices visited in order.
6. Prove using the Pigeonhole Principle that if I choose 10 points in a $3 \times 3$ square, two of them will be at distance $\leq \sqrt{2}$ from each other. Be sure to state the counting facts you use.
7. RSA problem

Your RSA key \( N = pq \) is 55 and your encryption exponent \( r \) is 3.

(a) Find your decryption exponent (Hint: it is the reciprocal of 3 in a certain modulus). Show all work.

(b) Decode the message 17. Show all work.
8. Factoring magic

(a) Prove this theorem: if \( p \) is a prime, and \( p \mid ab \), then either \( p \mid a \) or \( p \mid b \).

Your proof should not mention prime factorizations: it is the basis for the proof of the uniqueness of prime factorizations! It should use the basic theorem about greatest common divisors and the definition of divisibility. (another part on the next page)
(b) Use the theorem proved in part a to prove this theorem: if $3|x$ and $7|x$ then $21|x$.

I want you to use the theorem of the first part – nothing about prime factorizations. Further, you should explicitly use the definition of divisibility: this will help you see how to use the theorem of part a!