CSC 8-151 Discrete Mathematics for Computer Science

Sample Exam 10_{bin} April 26, 2016

_____

name

For credit on these problems, **you must show your work** and justify your answers. Closed book, closed notes, no cell phones or computers allowed. Calculators are allowed.

1. (7 pts.) a. Give the hexadecimal representation of: $(11001101)_2 + (101010100)_2$

b. Give the binary representation of 476_8

c. Give the hexadecimal representation of 271.

2. (10 pts.) For what values of n is $2^n < n!$? Prove this inequality, using the Principle of Mathematical Induction, and starting at the appropriate basis value.

3. (10 pts.) Prove, using the Principle of Mathematical Induction, that $5 \mid n^5 - n$ for all $n \geq 0$.

4. (3 pts. each) True or false? Justify your answer. (A correct answer is required for credit; the justification is worth 2 of the 3 points for each problem.)

_____a. $-a \cong a \bmod n$, for a and n positive integers.

_____b. $\phi(15) = 10$, where ϕ is the Euler phi function.

_____c. 210 has an inverse mod 441.

_____d. gcd(b,0)= 1, for b any positive integer.

_____e. The number 99! ends in exactly 22 zeros.

5. (10 pts.) a. Show that gcd(49, 13) = 1 using the Euclidean algorithm.

b. Find the inverse of 13 modulo 49 using your work from part a.

c. What part does this algorithm play in RSA/ public key encryption?

6. (10 pts.) a. Find 7^{12} mod 19 using repeated squaring/modular exponentiation. Show your work.

b. How many multiplications would be required to evaluate 322^{521} mod 777 using repeated squaring? Justify your answer without evaluating this expression.

c. What part does this algorithm play in RSA/ public key encryption?

7. (3 pts.) One of the key differences between traditional secret key encryption and modern public key encryption is that secret key is symmetric while public key is asymmetric. Explain the meaning of symmetric and asymmetric in this context.

8. (6 pts.) What is a "collision" when using a hashing function and how might it be resolved? (We discussed three, choose one of these to describe). Illustrate with an example (supply a hashing function, domain: students in our class, and codomain: memory locations between 0 and 99.) Is the hashing function you described one-to-one?

9. (5 pts.) Prove the following, using the definition of congruence modulo n:
If $a \equiv b(mod n)$ and $c \equiv d(mod n)$ then $(a + c) \equiv (b + d)(mod n)$

10. a. (3 pts.) Give the first sentence of Euclid's proof that there are infinitely many prime numbers.

11. Carefully prove the following:
$5n^2 + n + 7$ is $\mathcal{O}(n^2)$.

12. (3 pts. each) For which one of the growth functions, g(n), is f(n) $\Theta(g(n))$? **Briefly justify your answer.** For this problem choose among the following growth functions g(n): n, n^2, n^3, log n, n log n, 1, 2^n.

a. Let f(n) represent the worst case complexity of selection sort for a list of length n.

b. f(n) = n log n + 7n

c. Let f(n) represent the number of steps to determine set membership for a number when a set is implemented using a bit string.

d. The function f:N→N given by the rule f(n) = $\sum_{k=0}^{n}(k+1)$

13. True or false

True False c. x is $\mathbf{O}$(x log x).

True False d. If f(x) is $\mathbf{\Theta}$(g(x)) then f(x) is $\mathbf{O}$(g(x)).