Prof. Sergio A. Alvarez
21 Campanella Way, room 569
Computer Science Department
Boston College
Chestnut Hill, MA 02467 USA

http://www.cs.bc.edu/∼alvarez/
alvarez@cs.bc.edu
voice: (617) 552-4333
fax: (617) 552-6790

CS383, Algorithms
Spring 2009
HW2

1. Here is a very simple algorithm for computing the greatest common divisor of two integers:

   Algorithm 1: simpleGCD
   Input: Two integers $x \geq y > 0$.
   Output: The greatest common divisor of x and y.
   SIMPLEGCD(x, y)
   (1) **foreach** $d = y \cdots 1$
   (2) **if** $x \mod d = 0$ and $y \mod d = 0$
   (3) **return** d

   (a) Notice that Algorithm 1 makes at most y passes through the main loop. Also, the time required for each pass is dominated by the time spent in computing the modular remainders. Does this imply that Algorithm 1 is efficient, in the sense that its running time is bounded above by a polynomial in the input size? Explain.

   (b) Analyze the running time of Algorithm 1 in detail, explaining each step. Express your answer in asymptotic notation.

2. Let A denote an unspecified algorithm that operates on a collection of pixels as the input. We are interested in the worst-case asymptotic running time of A.

   (a) If A's running time is known to be $O(3^n)$, where n is the number of pixels in the input, is it still possible for A to have a polynomial running time? Explain.

   (b) If A's running time is known to be $\Omega(n^3)$, must its running time be $\Omega(n)$ also? Explain.

   (c) Assume that for each positive integer n there is a special "test image" I_n that contains exactly n pixels such that A's computation on input I_n requires exactly $17n^3$ basic steps. Based on this information alone, what is *the most specific* conclusion that can be reached regarding the asymptotic time complexity (running time) of A? Use asymptotic notation (O, Ω, Θ, as appropriate). Explain your answer carefully.

3. (a) Write out the full computation in tabular form for the extended Euclid gcd algorithm (as discussed in class) on input $(31, 12)$. The result of the computation should be three integers (x, y, d), where $d = \gcd(31, 12)$ and $x * 31 + y * 12 = 1$. Explain.

   (b) Based on the preceding subtask, what is the multiplicative inverse of 12 modulo 31? Explain.

(c) Suppose that x is a number such that $125 * x$ exceeds a multiple of 17 by exactly 1 (as do the numbers 18, 35, 52...). What is the remainder of x modulo 17? Explain.

4. Use the substitution rule of modular arithmetic to compute each of the following values. Include a step by step explanation and an answer in each case.

   (a) $55 * 973 \pmod{19}$

   (b) $251^{29} \pmod{3}$

   (c) $30^{11} + 2^{500} \pmod{25}$

5. Romeo's public RSA key is:

$$N = 1238231 \quad e = 806903$$

   Juliet wishes to send Romeo a secret message s, an uppercase text string describing one of her favorite things. She first encodes s as an integer m as follows: each character of s is converted to its numerical position in the alphabet ($A = 1$, $B = 2$, etc.) and the resulting string of numbers is interpreted as an integer value in base 32 positional notation. For example, the string "ABC" yields the integer value

$$1 * 32^2 + 2 * 32 + 3$$

   Juliet then sends the RSA-encrypted value of m below, using Romeo's public key:

$$m^e \bmod N$$

   Suppose you manage to intercept the encrypted value, which happens to be 510546. Can you break the code and recover Juliet's original message s?