Homework 1

Asymptotics and Number Theoretic Algorithms

Deadline: start of 7^{th} lecture (i.e., 10:20am, February 13, 2013).
Available points: 110. Perfect score: 100.

You will receive 10% extra credit points if you submit your answers as a typeset PDF (preferably using LaTeX, in which case you can also submit electronically your source code). Resources on how to use LaTeX are available on the course's website. Do not submit Word documents, raw text, etc. Make sure to generate and submit a PDF if you want to get the extra credit points. In this case you can submit your solutions electronically through `sakai.rutgers.edu`.

If you choose to submit handwritten answers and we are not able to read them, you will not be awarded any points for the part of the solution that is unreadable. Handwritten answer-sheets can be submitted to the instructor in class or to one of the TAs during office hours.

Try to be precise. Have in mind that you are trying to convince a very skeptical reader (and computer scientists are the worst kind...) that your answers are correct.

Each pair of students must write its solutions independently, without using common notes or worksheets with other students. You must indicate at the top of your homework who you worked with. You must also indicate any external sources you have used in the preparation of your solution. Make sure you do not violate any of the academic standards of the course, the department or of the university (available through the course's website)

Problem 1:

A. Compute the asymptotic running time of the following algorithm as a function of N given:

- the running times of integer arithmetic operations discussed in the class;
- that $s = O(logN)$;
- the running time of `Random_Integer`$(\cdot, \cdot)$ is O(1).

Algorithm 1: `MR_Function` (an odd integer N, integer s)

```
1  express N − 1 as 2^t · u where u is odd;
2  for i ← 1 to s do
3      a ← Random_Integer(2, N − 2);
4      if EuclidGCD(a, N) ≠ 1 then
5          return FALSE;
6      x_0 ← a^u mod N;
7      for j ← 1 to t do
8          x_j ← x_{j−1}^2 mod N;
9          if x_j = 1 and x_{j−1} ≠ 1 and x_{j−1} ≠ N − 1 then
10             return FALSE;
11     if x_t ≠ 1 then
12         return FALSE;
13 return TRUE;
```

B. Include the resulting running time of the above algorithm in the following list and order the resulting set of functions given their asymptotic growth. If $f_i(n) = \Theta(f_j(n))$ then the two functions should be given the same rank. Justify pairwise your ordering.

- $f_1(n) = n^3$
- $f_2(n) = n!$
- $f_3(n) = nlog_2n$
- $f_4(n) = 1$
- $f_5(n) = 2^{log_2n}$
- $f_6(n) = 10nlog_{10}n$
- $f_7(n) = (n+1)!$
- $f_8(n) = 4^{log_2n}$
- $f_9(n) = n^{log_2log_2n}$
- $f_{10}(b) =$ the running time of the algorithm in problem 1A.

(20 points)

Problem 2:

A. Consider a large number N in a binary and a decimal representation. What is the ratio of the number of bits over the number of decimal digits needed to express the number in the two representations?

B. Consider the following multiplication rule, where x has m bits and y has n bits. What is the running time of computing the product according to this rule?

$$x \cdot y = \begin{cases} 2(x \cdot \lfloor \frac{y}{2} \rfloor), & y : even \\ x + 2(x \cdot \lfloor \frac{y}{2} \rfloor), & y : odd \end{cases}$$

(10 points)

Problem 3:
A. Compute the following:

- What is 2^{2013} mod 3?
- Find the (modulo multiplicative) inverse of: 20 mod 79, 3 mod 62, 21 mod 91, 5 mod 23.

B. Assume that $m = x^{-1} \mod y$. Is there then an integer n so that $n = y^{-1} \mod x$? Prove or disprove.
(15 points)

Problem 4:

A. Assume two positive integers $x < y$. What is the relationship between $gcd(x+y, x+2y)$ and $gcd(x, y)$?

B. The Lucas numbers are defined as follows:

$$L_n = \begin{cases} 2 & if n = 0; \\ 1 & if n = 1; \\ L_{n-1} + L_{n-2} & if n > 1; \end{cases}$$

The sequence of Lucas numbers begins as follows: 2, 1, 3, 4, 7, 11, 18, 29, 47, 76 . . . Prove that any two consecutive terms of the Lucas sequence are relatively prime.
(10 points)

Problem 5:

A. Make a table with three columns. The first column is all numbers from 0 to 16. The second is the residues of these numbers modulo 5; the third column is the residues modulo 7.

B. Consider two different prime numbers x and y. Show that the following is true: for every pair of numbers m and n so that: $0 \leq m < x$ and $0 \leq n < y$, there is a unique integer q, where $0 \leq q < xy$, so that:

$$q = m \ mod \ x \quad \text{as well as} \quad q = n \ mod \ y$$

[Hint: Think how many q's in the range $[0, xy]$ can have the same result modulo x and modulo y and count how many q's there are.]

C. The previous problem asks to go from q to (m, n). It is also possible to go the other way. In particular, show the following:

$$q = \{m \cdot y \cdot (y^{-1} \ mod \ x) + n \cdot x \cdot (x^{-1} \ mod \ y)\} \mod mn$$

[Hint: Ensure that if the above is true then the expressions in 5A are also true. Consider the values of the following terms: $c_x = y \cdot (y^{-1} \ mod \ x)$ and $c_y = x \cdot (x^{-1} \ mod \ y)$ and their values $mod \ x$ and $mod \ y$.]

D. What happens in the case of three primes x, y and z? Do the above properties still hold? If they do, how do they look like in this case?
(20 points)

Problem 6:

Andrew transmitted an n-bit message x to Amr, Abdul and Matthew, using RSA, i.e., he used the public keys of his friends (N_i, e) to encode the message and transmitted three encrypted versions of the original message y_1, y_2, y_3, once to each recipient. All of Andrew's friends used the exponent $e = 3$ so as to speed up the modular exponentiation process.

Kostas managed to intercept all three encrypted messages and recover the original message. What algorithm did Kostas use?

[Hint: Consider how the three transmitted messages are computed. Have in mind that the symmetric property holds for modulo arithmetic. Be careful with the details and under which conditions you apply certain expressions.]
(15 points)

Problem 7:

Consider a family of hash functions $\mathcal{H}$ from a finite set X to a finite set Y, that has the following property: $Pr\{h(m) = h(n)\} \leq p$, where the actual hash function h is selected randomly from the set $\mathcal{H}$ and m, n are distinct elements in X. Show that there is a lower bound for the value p. In particular, that $p \geq \frac{|X|-|Y|}{|Y| \cdot (|X|-1)}$, where $|X|$ and $|Y|$ correspond to the number of elements in the sets X and Y correspondingly.

[Hint: What is the expected number of elements from X mapped to each entry of $|Y|$?]
(20 points)