Problem Set 1

CPSC 629 Analysis of Algorithms

Andreas Klappenecker

The assignment is due next Tuesday (09/17/2002), before class.

Image that you work as a consultant for NASA. The following algorithm was included by Dr. T. Ricky in the LUNA' program. Your job is to prove that the following algorithm meets its specifications.

Input: An odd integer x, $0 < x < 2^w$.
Output: An integer y such that $xy \equiv 1 \bmod 2^w$.

1: y := 1;
2: **for** $i = 2$ to w **do**
3:     **if** $2^{i-1} < xy \bmod 2^i$ **then** $y := y + 2^{i-1}$; **fi**;
4: **od**;
5: **return** y.

Q1 What standard algorithm could be used to solve this problem? Give a concise but full explanation.

Q2 What is the (runtime) bit complexity of the above algorithm. How does this compare to the bit complexity of your algorithm in Q1. Use big Oh notation. [Assume classical multiplication in both cases.] Which algorithm is preferable from a practical point of view?

Q3 List the values of the variables x, y, 2^i after each iteration (after line 3) for the input $x = 11$ and wordlength $w = 5$.

Q4 Show that you are worth your money and prove that the algorithm is correct. What property is invariantly true at the end of line 3?

Hint: Dr. T. Ricky was not available. However, you could talk to the slightly odd system administrator S.M. Elly. He did not seem to be particularly helpful, and apparently had not had any contact with humans in a long, long time. He merely uttered "It is an odd fact that x is odd, really, really odd...In the product of x and y is the clue, that much is true...". The more you think about it, Elly seems to be right.

Q5 Construct the finite field $\mathbf{F}_9$ with 9 elements. Use a sparse irreducible polynomial if that is possible.

Reading Assignment: Study the lecture notes on Groups, Rings, and Finite Fields.