Advanced Algorithms

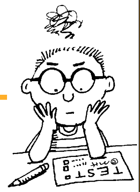
Floriano Zini

Free University of Bozen-Bolzano
Faculty of Computer Science

Academic Year 2013-2014

Lab 3 – Solutions of assignment

Assignment 02



Exercise 1.28 page 40 DPV

- In an RSA cryptosystem, *p* = *7* and *q* = *11*. Find appropriate exponents *d* and *e*.

Solution

- We first calculate (p−1)*(q−1) which in our case is 6*10=60.
  Then we need to come up with an *e* which is relatively prime to 60 so that it has an inverse d. We observe that e = 11 has gcd(11, 60) = 1 and 11*11=1 mod60, therefore the values e=11 and d=11 are appropriate.
  Other good pairs are (7, 43), (13, 37), (17, 53), (19, 59), (23, 47), (29, 29), (31, 31), (41, 41).

Assignment 02 (cont.)

Exercise 1.33 page 41 DPV

- Give an efficient algorithm to compute the *least common multiple* of two *n*-bit numbers *x* and *y*, that is, the smallest number divisible by both *x* and *y*. What is the running time of your algorithm as a function of *n*?

Solution

- The least common multiple (lcm) of any two numbers x,y can easily be seen to equal lcm(x,y) = (x*y)/ gcd(x, y). We therefore need O(n^3) operations to compute the gcd, O(n^2) operations to multiply x and y and O(2*n*n) = O(n^2) operations to divide. Total O(n^3) running time

Assignment 02 (cont.)

Exercise

- Implement in Octave the algorithm you have found in the previous exercise to calculate the least common multiple

```
function g = lcm(a,b)
g=a*b/gcd(a,b);
end
```