Home Work 2

msk

February 27, 2015

Problem 1.11

$(4^1536) mod 35$ Since 35 is a product of two primes 5 and 7

we know by Euler's theorem, we have $4^{4\times6} mod 35 = 1$

Since 1536 is multiple of 24, we have $4^{1536} mod 35 = 1$

Similarly $9^{24} mod 35 = 1$. Since 4824 is a multiple of 24, we have $9^{4824} mod 35$ =1.

Hence their difference is 0.

Problem 1.13

$5^{30} mod 31 = 1$ by Fermat's Little Theorem.

Since 30,000 is a amultiple e of 30, we have $5^{30000} mod 31 = 1$

Similarly $6^{30} mod 31 = 1$. Since 123456 mod 30 is 6.

$6^6 mod 31$ is $6^3 mod 31$ = -1 Hence $6^6 mod 31$ is 1.

Hence the difference of 5^{30000} and 6^{123456} is 0 mod 31 or the differenc eis divisible by 31.

Problem 1.16

Computing x^{62} Repeated Squaring method $x^{31} * x^{31}$, $x^{15} * x^{15} * x$, $x^7 * x^7 * x$, $x^3 * x^3 * x$, $x * x * x$ takes 1+2+2+2+2=9 multiplications.

However if we do $x * x$,$x^2 * x^2 * x$, $x^5 * x^5 * x^5$,$x^{15} * x^{15} * x$,$x^{31} * x^{31}$ takes 1+2+2+2+1=8 multiplications.

Computing s^{124} requires 10 multiplications by repeated squaing.

However x^{124} requires only 9 multiplications (similar to how we computed X^{62}/

Problem 1.17

Iterative Algorithm requires y-1 iterations. In each iteration the size of one of the operands increase. So the total complexity will be $O(n^2 + 2n^2 + 3n^2 + ... + (y-1)n^2)$. So the complexity is $O(y^2n^2)$

Repeated squaring takes $log(y)$ iterations. In each iteration the size of both operands increase. So the total comlexity is $O(n^2 + 2^2n^2 + 2^4n^2 + ... +$

$2^{\lfloor log(y)-1 \rfloor} n^2)$ giving rise $O(y^2n^2)$ Both the algorithms have the same running time in bit complexity.

Problem 4

inverse of 19 mod 79

```
79 19 4 3
19 3  6 1
3  1  3 0
1 0
1 = 1-0 = 1*1-(1*3-3*1) = 4*1 - 1*3 = 4 * (1*19 - 6*3) - 1*3
  = 4 *19 - 25*3 = 4*19 - 25 * ( 1*79 - 4*19) = 104 * 19 - 25*79

Hence the inverse is 25
```

inverse of 22 mod 91

```
91 22 4 3
22 3  7 1
3  1  3 0
1 0

1 = 1 - 0 = 1 - (3- 3*1) = 4*1 - 1*3 = 4 *( 22 - 7*3) - 1*3
 = 4 * 22 - 29 *3 = 4 *22 - 29* (91-4*22) = 120*22 - 29*91
hence the inverse is  29.

inverse 3 mod 62 is 21
```

inverse of 7 mod 23

```
23 7 3 2
7 2  3 1
2 1  2 0
1 0

1 = 1-0 = 1- (2-2*1) = 3*1 - 2 = 3 * (7-3*2) - 2 = 3*7 -10*2
 = 3*7 - 10*(23-3*7) = 33*7 -10*23
Hence the inverse of 7 mod 22 is 10
```

5

$19^{19^{19}}$ *mod* 10 **We know** 19^4 **is 1 as 10 =2 * 5**

To calulate 19^{19} *mod* 4 **is -1= 3 and hence the least significant digit (mod 10) is 9.**

$3^{5^{2015}}$ *mod* 7 **We know** 3^6 **is 1 by FLT**

To calulate 5^{2015} *mod* 6 **is -1= 5 and hence** 3^5 **mod 7 is 5.**

Problem 6

p =23 q = 29 N =667 e = 3

d is the inverse of e mod (22*28 = 616) which (p-1)* (q-1)

Obtained using Extended Euclidean Algorithm

```
616 3 205 1
3 1   3   0
1 0

1 = 1-0 = 1- (3-3*1) = 4*1 - 3 = 4* (616- 205*3) - 3 = 4*616 - 821*3

inverse is 411 mod 616.

d = 411

encrypted messge 341 ^ 3 mod 667 = 5 (using modexp algorithm from Lab)
```

Problem 2.4

a. $T(n) = 5T(n/2) + cn$

To solve this recurrence equation, we can use Master Theorem a = 5, b= 2, d= 1, and $a > b^2$ **, we get** $T(n) = n^{log_2(5)}$ **which is** $O(n^{2.32})$

b. $T(n) = 2T(n-1) + c$

By Telescoping method we can solve this recurrence.

Solving this we get $O(2^n)$

c. $T(n) = 9T(n/3) + n^2$

To solve this you can use Master Theorem a = 9, b = 3 d = 2 and $a = b^d$ **so we get** $T(n) = O(n^2\ log(n)$

So we prefer algorithm c.

Problem 2.5 c, d and e

a. $T(n) = 7T(n/7) + n$

Using Master Theorem a = 7 b =7 d = 1 $a = b^d$ **we get**

$T(n) = \Theta(n^log(n))$

d. $T(n) = 9T(n/3) + n^2$

Using Master Theorem a = 9, b = 3, d =2 $a = b^d$ **we get**

$T(n) = \Theta(n^2log(n))$

e. $T(n) = 8T(n/2) + n^3$

Using Master Theorem a = 8, b =2, d = 3, $a = b^d$ **we get**

$T(n) = \Theta(n^3log(n))$

Problem 2.12

The number of lines printed is governed by the recurrence equation $T(n) = 2T(n/2) + 1$

with $T(2) = 1$

$T(4) = 2 * T(2) + 1 = 3$

Assuming $n = 2^k$, $T(2^k) = 2T(2^{k-1}) + 1$

Induction Hypoothesis T(k) = k-1 for k ¿1. Base case is True. Assume it is true for $k = 2^{i-1}$

$T(2^i) = 2 * (2^{i-1} - 1) + 1 = 2^i - 1$

For all $2^i < n < 2i + 1$ **the number of lines printed will be** $2^{i+1} - 1$

Number of lines printed will be $\Theta(n)$

Problem 2.13

Please see http://goo.gl/vaw2tz

Problem 4.1 a
$T(n) = T(\sqrt(n)) + 1$
Let $n = 2^{2^k}$**,** $\sqrt(n) = 2^{2^{k-1}}$
$T_1(k) = T_1(k-1) + 1$
So $T_1(k) = k$
$T(n) = \log(\log(n))$ **Problem 4.d**

$T(n) = T(n-1) + 1/n$
$T(n) = H(n)$ **where H(n) is a Harmonic number** $\sum_{i=1}^{n} i$ **and this is approximated by** $\log(n)$ **so** $T(n) = \log(n)$