算法设计与应用基础: Homework No 1

16337341 朱志儒

第一题

正确性:

当 x = 0 时，q = 0，r = 0，显然正确。

设上次递归返回的商为 q’，余为 r’。

a. 若 2r’ < y，则当 x 为奇数时，

$$x = [x/2] * 2 + 1 = 2(q'y + r') + 1 = 2q'y + 2r' + 1$$

即 q = 2q’，r = 2r’ + 1。

当 x 为偶数时，

$$x = [x/2] * 2 = 2q'y + 2r'$$

即 q = 2q’，r = 2r’。

b. 若 2r’ >= y，则当 x 为奇数时，

$$x = [x/2] * 2 + 1 = 2(q'y + r') + 1 = 2q'y + 2r' + 1 = (2q' + 1)y + (2r' + 1 - y)$$

即 q = 2q’ + 1，r = 2r’ + 1 – y。

当 x 为偶数时,

$$x = [x/2] * 2 = 2q'y + 2r' = (2q' + 1)y + (2r' - y)$$

即 q = 2q’ + 1，r = 2r’ – y。

算法复杂度:

因为整数 x 是 n 位，所以该算法一共递归 n 次，每次递归中均要 O(n)次操作，则该算法的时间复杂度为 $O(n^2)$。

第二题:

迭代算法：$x^y = x * x^{y-1}$，共迭代 O(y)次，设迭代步数为 i，则在第 i 次迭代的

乘法时间复杂度为 $O(i * \log x * \log x)$，故总时间复杂度为 $O((y \log x)^2)$。

递归算法：$x^y = (x^{y/2})^2 * x^{y \bmod 2}$，共递归 $O(\log y)$次，设递归步数为 i，则在第 i 次递归的乘法时间复杂度为 $O(2^{i-1} * \log x * 2^{i-1} * \log x)$，故总时间复杂度为 $O(y(\log x)^2)$。

第三题：

因为 p = 7，q = 11，则 N = pq = 77，M = (p - 1)(q - 1) = 60，所以可找到一个与 M 互素的 e = 13，则 e 模 M 操作的逆 d = -83

Programming