477.1001/677.1001 Design and Analysis of Algorithms
University of Nevada, Las Vegas
Spring 2020
Assignment 6
Due: Saturday, March 14, 2020, by email

1. Draw a binomial (max)-heap that contains the elements `1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15`. The element 15 has to be in tree B_3. Perform a Delete_Max operation on this heap.

2. Binomial Heap H_1 consists of binomial trees: B_0, B_1, B_2, B_3. Binomial Heap H_2 consists of binomial trees: B_0, B_3, B_4. Binomial Heaps H_1 and H_2 are merged into H. What are the binomial trees of H?

3. Show the steps of radix sort for the following sequence. Use counting sort to sort single digits.

   `22 34 7 88 3 66 71 94 15`

4. Insert the following IP addresses into a hash table of size 5 using universal hashing with $a_1 = 1$, $a_2 = 2$, $a_3 = 4$ and $a_4 = 5$:

   - 209.85.231.104 Google
   - 207.46.170.123 Microsoft
   - 208.80.152.2 Wikipedia

5. What does the randomized primality testing algorithm (based on the little Fermat theorem) return for $n = 281$ and $a = 2$? Is it "yes" (*i.e.* prime) or "no" (*i.e.* composite)?

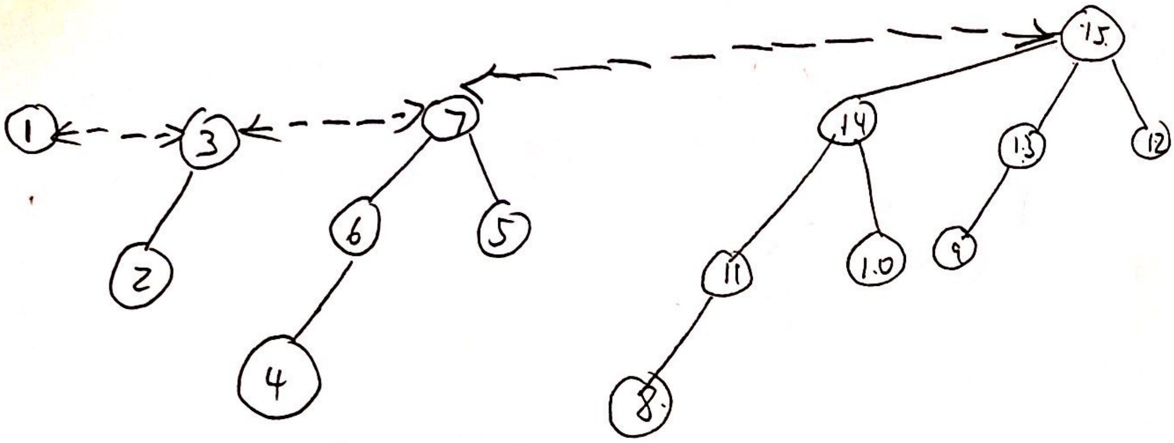
6. Consider the RSA encryption scheme. Bob chooses prime numbers $p = 17$ and $q = 19$, and publishes his key as $n = 323$ and $e = 287$. What does Alice send to Bob, if she wants to communicate 2?

How to submit. Create one PDF file with your solutions. Email this file as an attachment to the TA, Mahdi Hajiali, Hajiali@unlv.nevada.edu. Subject of your email must be

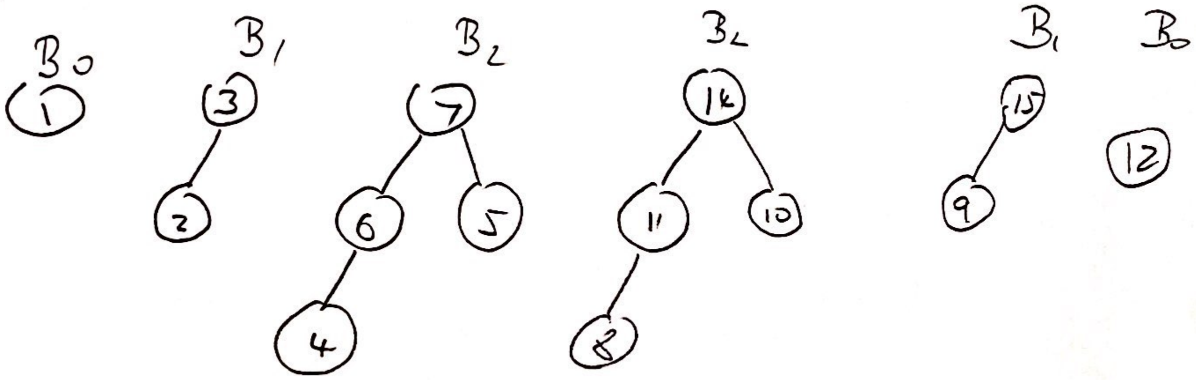
`CS477 Bein Assignment 6, <your name>, <your student ID number>.`

Asgn 6 Solutions

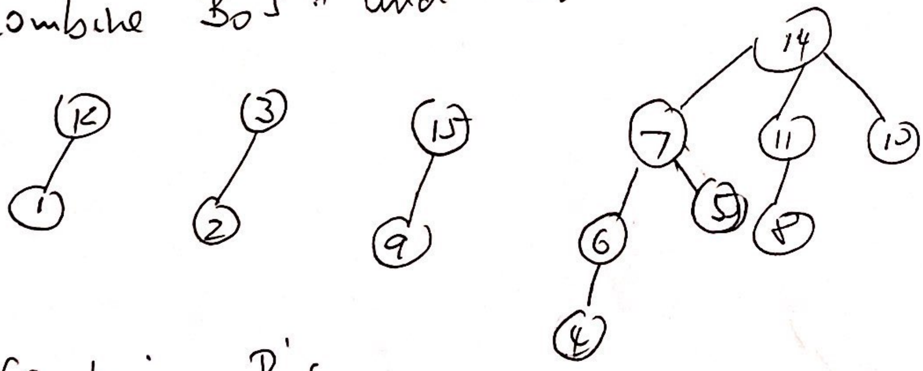
5 :



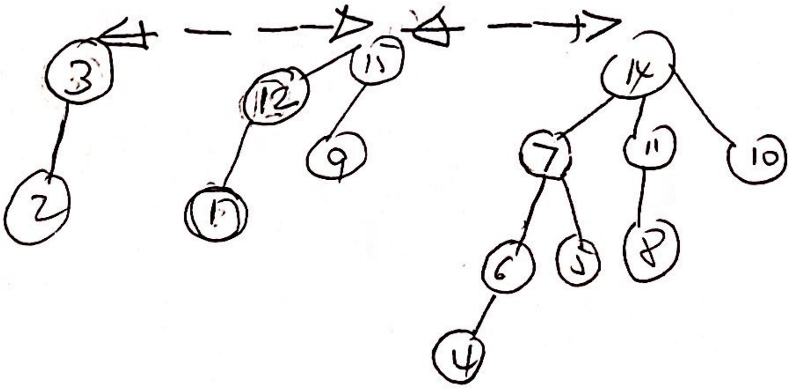
delete 15



combine B0's and B2's



Combine B1's



Result

2]

B_0	B_1	B_2	B_3	–	
B_0			B_3	B_4	
	B_1	B_2	B_3	B_4	
–	–	–	B_3	–	B_5

B_3, B_5

3]

22 34 07 88 03 66 71 94 15

Sort by last digit

counting sort

Count array:

0	1	1	1	2	1	1	1	1	0
0	1	2	3	4	5	6	7	8	9

accumulated count array:

				−1	−1				
0	1	2	3	5	6	7	8	9	9
0	1	2	3	4	5	6	7	8	9

now insert into places

71	22	03	34	94	15	66	07	88
1	2	3	4	5	6	7	8	9

Sorted:

71 22 03 34 94 15 66 07 88

repeat for first digit, result is:

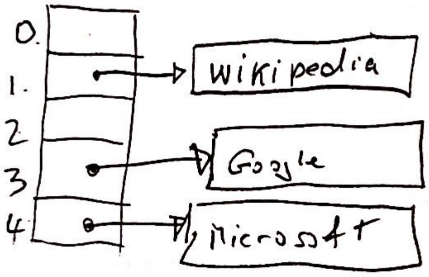
03 07 15 22 34 66 71 88 94

4]

$209*1 + 85*2 + 231*4 + 104*5 = 1823 \bmod 5 = 3$

$207 \quad 46 \quad 170 \quad 123 = 1594 \bmod 5 = 4$

$208 \quad 80 \quad 152 \quad 2 = 986 \bmod 5 = 1$



5]

$2^{280} \bmod 281 = 1$ (using Wolfram Alpha)

or:

$2^{10} \bmod 281 = 181 \Rightarrow 2^{40} \bmod 281 = (181)^4 \bmod 281$

$= 249$

$2^{280} \bmod 281 = (249)^7 \bmod 281$

$= 1$

5.

$p = 17 \quad q = 19 \quad e = 287$

a) $z = pq = 323$ $\quad n \cdot s \bmod (p-1)(q-1) = 1$

$\rightarrow s = 287$

b) a) Alice sends $2^{287} \bmod 323 = 162$

b) ~~Bob decrypts 33^{287} mod 323 = 186~~