CS 3333 Mathematical Foundations Spring '11

Recitation 4 & 5 Practiced on: 1/31 & 2/2 5:30 - 6:20 pm

Integers and Algorithm

Note: These problems are designed for practice during a 50 minute recitation.

a) **Easy** problems: expected to be solved in *5 min*.
b) **Medium** problems: expected to be solved in *30 min*.
c) **Hard** problems: expected to be solved in *15 min*.

During the recitation, you may discuss the problems with your peers and the TA. Please control your volume and don't annoy others. An electronic copy of these problems and solutions will be posted on the following URL: http://cs.utsa.edu/~btang/pages/teaching.html.

Solutions:

1. (3 min) Convert these integers from decimal notation to binary notation. (Textbook [KR] Page 229: 1 a & b)

   a) 231.
   Answer: we can compute that $2^0 + 2^1 + 2^2 + 2^5 + 2^6 + 2^7 = 231$. So $(231)_{10} = (1110\ 0111)_2$.

   b) 4532.
   Answer: we can compute that $2^2 + 2^4 + 2^5 + 2^7 + 2^8 + 2^{12} = 4532$. So $(4532)_{10} = (1\ 0001\ 1011\ 0100)_2$.

2. (2 min) Convert these integers from hexadecimal notation to binary notation. (Textbook [KR] Page 229: 5 a & b)

   a) 80E.
   Answer: $(80E)_{16} = (1000\ 0000\ 1110)_2$.

   b) 135AB.
   Answer: $(135AB)_{16} = (0001\ 0011\ 0101\ 1010\ 1011)_2$.

3. (10 min)Use *Algorithm 5* to find 7^{644} mod 645. (Textbook [KR] Page 230: 19, hint: Page 226-227)
   Answer: Since $644 = (10\ 1000\ 0100)_2$, we need to multiply together 7^4 mod 645, 7^{128} mod 645, 7^{512} mod 645, reducing modulo 645 at each step. We compute by repeatedly squaring: 7^2 mod 645 = 49, **7^4 mod 645 = 49^2 mod 645 = 466**, 7^8 mod 645 = 466^2 mod 645 = 436, 7^{16} mod 645 = 436^2 mod 645 = 466. At this point we see a pattern with period 2, so we have 7^{32} mod 645 = 436, 7^{64} mod 645 = 466, **7^{128} mod 645 = 436**, 7^{256} mod 645 = 466, **7^{512} mod 645 = 436**. Thus our final answer will be the product of 466(equals to 7^4 mod 645), 436(equals to 7^{128} mod 645) and 436(equals to 7^{512} mod 645), reduced modulo 645. We compute these one at a time: $466 \cdot 436$ mod 645 = 1, and $1 \cdot 436$ mod 645 = 436. So 7^{644} mod 645 = 436.

Bo Tang
Mail: CS Department, UT San Antonio, San Antonio TX 78249, USA
Phone: 210-458-5592 Email: btang[at]cs.utsa.edu Homepage: http://cs.utsa.edu/~btang/

CS 3333 Mathematical Foundations Spring '11

Recitation 4 & 5 Practiced on: 1/31 & 2/2 5:30 - 6:20 pm

Integers and Algorithm

4. (10 min)Use the Euclidean algorithm to find: (Textbook [KR] Page 230: 23 e & f)

   a) gcd(1000,5040).
   Answer: gcd(5040, 1000) = gcd(1000, 40) = gcd(40, 0) = 40.

   b) gcd(9888,6060).
   Answer: gcd(9888, 6060) = gcd(6060, 3828) = gcd(3828, 2232) = gcd(2232, 1596) = gcd(1596, 636) = gcd(636, 324) = gcd(324, 312) = gcd(312, 12) = gcd(12, 0) = 12.

5. (10 min)Multiply $(1110)_2$ and $(1010)_2$ by working through each step of the algorithm for multiplication given in the text. (Textbook [KR] Page 231: 50, Hint: Page 224-225)
   Answer: The partial products are 11100 and 1110000, namely 1110 shifted one place and three places to the left. We add these two numbers, obtaining 10001100.

6. (15 min)How many bit operations does the comparison algorithm from Exercise 53 use when the larger of a and b has n bits in its binary expansion? (Textbook [KR] Page 231: 54 , hint: use the algorithm given in the answers section, page S-22, of the textbook)
   Answer: In the worst case, each bit of a has to be compared to each bit of b, so O(n) comparisons are needed. An exact analysis of the procedure given in the solution to Exercise 53 shows that n+1 comparisons of bits are needed in the worst case, assuming that the logical "and" condition in the **while** loop is evaluated efficiently from left to right (so that a_0 is not compared to b_0 there).

   Reference: solution pseudo-code for Exercise 53:

```
1  procedure compare(a, b: nonnegative integers)
2  i := n – 1
3  while i > 0 and a_i = b_i
4        i := i – 1
5  if a_i > b_i then answer := "a > b"
6  else if a_i < b_i then answer := "a < b"
7  else answer := "a = b"
8  {the answer is recorded in answer}
```

Bo Tang
Mail: CS Department, UT San Antonio, San Antonio TX 78249, USA
Phone: 210-458-5592 Email: btang[at]cs.utsa.edu Homepage: http://cs.utsa.edu/~btang/