MAT2440 Practice Exam Solutions 3 Halleck Spring 2018

* Book and notes are prohibited except for a single sheet (back and front) with hand-written formulae/notes. Submit formula sheet with your exam for up to 5 extra points.
* You may write on test page. However, put all your work and answers into the blue book.
* No credit will be given for any answer that is not backed up with work.
* Problems marked \* require that part of the work be done in MS Excel. Please submit a single Excel file on Blackboard at the end of the exam. Create a tab for each problem that uses Excel.
1. Let *a* ≠ 0, *b*, and *c* be integers. Show that if *a*|*b* and *a*|*c*, then *a*|(*b* + *c*).

***b* = *ka* and *c* = *ma*, so *b*+*c* = *ka* + *ma* = (*k*+*m*)*a*. \ *a*|(*b* + *c*)**

1. \*Convert 3452 to: **(see excel file for work)**

(a) base 2

(b) base 3

(c) base 7

1. Convert the following number (ABBA)16 from hexadecimal to octal. Each character gets replaced by 2 characters according to the following chart:

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| hex | 0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | A | B | C | D | E | F |
| octal | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 1 |
|   | 0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 |

**So (12 13 13 12)8**

1. Find 32003 mod 99. Trying Excel: =MOD(3^2003, 99) we get an overflow error. We think carefully about what we are doing. We are dividing 32003 by 99 and finding its remainder. As a fraction, both numerator and denominator are divisible by 32=9, and we get the equivalent problem of 32001 mod 11. If we try Excel =MOD(3^2001,11), we again get an overflow error. But we are now working modulo 11, which is a prime and since 3 is not divisible by 11, Fermat’s little theorem applies. 11 − 1 = 10 so a power of 3 raised to a multiple of 10 evaluates to 1. Dividing 2001 by 10 gives a remainder of 1. Hence, this power evaluates to 3.
2. \*Use the Euclidean algorithm to find **(see excel file for work)**

(a) gcd(12; 18) **6**

(b) gcd(111; 201) **3**

(c) gcd(345; 346) **1**

(d) gcd(1005; 475) **5**

1. \*Which memory locations are assigned by the hashing function h(k) = k mod 97 to the records of insurance company customers with these Social Security numbers? **(see excel file for work)**

(a) 034-56-7981 **91**

(b) 220-19-5744 **21**

(c) 183-21-1232 **57**

1. Give Q estimates for each of these functions.
	1. *n* log*(n*2 + 1*)* + *n*2 log *n* **∈ Q(*n*2 log *n*)**
	2. *(n* log *n* + 1*)*2 + *(*log *n* + 1*)(n*2 + 1*)* **∈ Q(*n*2(log *n*)2)**
	3. $n^{2^{n}}+n^{n^{2}}$ **∈ Q(**$n^{2^{n}}$**)** (compare the exponents 2*n* and *n*2, since the base of *n* is the same)
2. Let *f*1*(x)* and *f*2*(x)* be functions from the set of real numbers to the set of positive real numbers. Show that if *f*1*(x)* and *f*2*(x)* are both Q*(g(x))*, where *g(x)* is a function from the set of real numbers to the set of positive real numbers, then *f*1*(x)* + *f*2*(x)* is Q *(g(x))*. Is this still true if *f*1*(x)* and *f*2*(x)* can take negative values?

***f*1*(x)* and *f*2*(x)* Q*(g(x))* and positive Þ ∃ m, n, p, q, r, s ∈ R+ such that**

**p g(x) ≤ *f*1*(x)* ≤ q g(x) ∀x > m and r g(x) ≤ *f*2*(x)* ≤ s g(x) ∀x > n.**

**Let t=p+r and u=q+s and choose k= max(m, n), then**

**t g(x) ≤ *f*1*(x) + f*2*(x)* ≤ u g(x) ∀x > k,**

**i.e., *f*1*(x)* + *f*2*(x)* is Q *(g(x)).***

**If positivity was not required, choose *f*2*(x)=− f*1*(x)***

**Then statement would be true only if g(x) was identically 0 beyond some point.**

**Otherwise *f*1*(x)* + *f*2*(x)* would be identically 0, and hencewould be O *(g(x))* but not *Ω (g(x)).***

1. What is the effect in the time required to solve a problem when you double the size of the input from *n* to 2*n*, assuming that the number of milliseconds the algorithm uses to solve the problem with input size *n* is each of these functions? Express each answer in simplest form possible, either as a ratio or a difference: may be a function of *n* or a constant.

**a)** log log *n* **b)** log *n* **c)** 100*n* **d)** *n* log *n* **e)** *n*2 **f )** *n*3**g)** 2*n*

**a) difference: log log 2n − log log n = log [(log 2n)/(log n)] Using calculus, the input into the outer log goes to 1 as n gets large (for those without calculus, check using Excel & big values for n). Hence entire expression goes to 0 as n gets large.**

**b) difference: log 2n − log n = log 2**

**c) ratio: 100(2n)/100n=2**

**d) ratio: 2*n* log 2*n/ (n* log *n)=*2*(*log 2*n/* log *n)=*2(see answer to a for explanation). Hence, the presence of the log does not affect result for large n.**

**e) ratio: 4 *n*2 /*n*2= 4**

**f) ratio: 8 *n*3 /*n*3= 8**

**g) ratio: 2*2n*/2*n* = 2*n***

1. Determine the least number of comparisons, or best-case performance,
	1. required to find the maximum of a sequence of *n* integers, using Algorithm 1 of Section 3.1.

**There are n-1 comparisons within loop plus the n bookkeeping for loop so 2n-1**

* 1. used to locate an element in a list of *n* terms with a linear search.

**If item is located in the first spot, then only the two comparisons are made within the first pass in the while condition. Another comparison is made outside loop so 3 in total.**

* 1. used to locate an element in a list of *n* terms using a binary search.
	2. **There are élog nù passes in loop plus 1 to exit loop and 1 outside loop. So 2(élog nù+1) in total**
1. **\***Explain why both 3792 and 2916 would be bad choices for the initial term of a sequence of four-digit pseudorandom numbers generated by the middle square method.

**(see excel file for work) 3792 results in a sequence of size 1. Every number generated is the same. 2916 results only in a sequence of size 4 before it starts repeating.**

1. **\***The ISBN-10 of *Elementary Number Theory and Its Applications* is 0-321-500Q1-8, where *Q* is a digit. Find the value of *Q*.

**Using Excel, we find that we get** $8Q+6≡0 mod 11$ **and if we substitute 1,…,10 into the left hand side, we see that Q = 9. Alternatively, use the Euclidean algorithm and back substitution to find an inverse of 8 and then multiply both sides of** $8Q≡-6 ≡5 mod 11$ **to get Q.**

1. **\***Encrypt the message WATCH YOUR STEP by translating the letters into numbers, applying the given encryption function, and then translating the numbers back into letters.
2. *f (p)* = *(p* + 14*)* **mod** 26
3. *f (p)* = *(*11*p* + 21*)* **mod** 26
4. *f (p)* = *(*−7*p* + 1*)* **mod** 26
5. **\***Suppose that the most common letter and the second most common letter in a long ciphertext produced by encrypting a plaintext using an affine cipher *f (p)* = *(ap* + *b)* **mod** 26 are Z and J, respectively. What are the most likely values of *a* and *b*?

**The most common letter is “E” and if it is mapped to “Z” then** $a4+b≡25 mod 26$**. Similarly, “T” is the 2nd most common letter, so we get**$ a19+b≡9 mod 26$ **Subtracting, we get** $15a≡-16 mod 26$ **or** $15a≡10 mod 26$ **Using Excel, we find that a = 18 and hence,** $b≡25-4\left(18\right)≡-47≡5 mod 26$ **See Excel for the check. Note that this would NOT be an actual cipher since a =18 is NOT relatively prime to 26. Only half the letters could appear in the cipher text and the plain text would not be readily recovered (see Excel file).**

1. **\***Decrypt the message EABW EFRO ATMR ASIN which is the ciphertext produced by encrypting a plaintext message using the transposition cipher with blocks of four letters and the permutation *σ* of {1*,* 2*,* 3*,* 4} defined by *σ(*1*)* = 3, *σ(*2*)* = 1, *σ(*3*)* = 4, and *σ(*4*)* = 2. **BEWARE OF MARTIANS**