MTH150 Midterm Exam 2 Solutions

November 9, 2006

A1 (a) $A \cup B = \{0, 1, 2, 3, 4, 5, 6\}$
(b) $A \cap B = \{3\}$
(c) $A - B = \{1, 2, 4, 5\}$
(d) $B - A = \{0, 6\}$

A2 (a) $f(n) = 2n$
(b) $f(n) = \lfloor n/2 \rfloor$
(c) $f(n) = \begin{cases} n+1 & \text{if } n \text{ is even} \\ n-1 & \text{if } n \text{ is odd} \end{cases}$
(d) $f(n) = 0$

A3 (a) (i) $3 \cdot 2^n$, $n \in \mathbb{N}$
(ii) $3n$, $n \in \mathbb{Z}^+$
(b) (i) $\sum_{i=1}^{2}\sum_{j=1}^{3}(i+j) = \sum_{i=1}^{2}((i+1)+(i+2)+(i+3)) = \sum_{i=1}^{2}(3i+6) = (3 \cdot 1 + 6) + (3 \cdot 2 + 6) = 21$
(ii) $\sum_{i=1}^{2}\sum_{j=1}^{3} ij = \sum_{i=1}^{2}(i \cdot 1 + i \cdot 2 + i \cdot 3) = \sum_{i=1}^{2} 6i = 6 \cdot 1 + 6 \cdot 2 = 18$

B1

i	j	a_1	a_2	a_3	a_4	a_5
		3	1	5	7	4
1	1	1	3	5	7	4
1	2	1	3	5	7	4
1	3	1	3	5	7	4
1	4	1	3	5	4	7
2	1	1	3	5	4	7
2	2	1	3	5	4	7
2	3	1	3	4	5	7
3	1	1	3	4	5	7
3	2	1	3	4	5	7
4	1	1	3	4	5	7

B2 (a) For any $C > 2$, it is possible to find a corresponding k. For $C = 3$, $k = 2$ is the smallest k that works. As in the proof of Theorem 1 (p. 184), $C = 8$ and $k = 0$ also work.
(b) Proceed by contradiction. Assume there exist C and k such that $n^3 \le Cn^2$ for $n > k$. Thus, if $n \ne 0$, we have $n \le C$ for $n > k$. However, this fails for large values of n such as $n = |C| + |k| + 1$.

B3 $\sum_{i=1}^{n-1}\sum_{j=1}^{n-i} 1 = \sum_{i=1}^{n-1}(n-i) = \sum_{i=1}^{n-1} n - \sum_{i=1}^{n-1} i = (n-1)n - \frac{(n-1)n}{2} = \frac{(n-1)n}{2}$

C1 (a) i. $13 \textbf{ mod } 3 = (4 \cdot 3 + 1) \textbf{ mod } = 1$

ii. $-97 \textbf{ mod } 11 = (-9 \cdot 11 + 2) \textbf{ mod } = 2$

(b) i. List the primes p satisfying $2 \le p \le \sqrt{193}$: $2, 3, 5, 7, 11, 13$. Check each prime until you find a divisor: $193 = 96 \cdot 2 + 1$, $193 = 64 \cdot 3 + 1$, $193 = 38 \cdot 5 + 3$, $193 = 27 \cdot 7 + 4$, $193 = 17 \cdot 11 + 6$, $193 = 14 \cdot 13 + 11$. There are no prime divisors so 193 is prime, i.e. the prime factorization of 193 is $193 = 193^1$.

ii. List the primes p satisfying $2 \le p \le \sqrt{1001}$: $2, 3, 4, 5, 7, 11, 13, 17, 19, 23, 29, 31$. Check each prime until you find a divisor: $1001 = 500 \cdot 2 + 1$, $1001 = 333 \cdot 3 + 2$, $1001 = 200 \cdot 5 + 1$, $1001 = 143 \cdot 7 + 0$. So 7 is a divisor.
List the primes p satisfying $7 \le p \le \sqrt{143}$: $7, 11$. Check each prime until you find a divisor: $143 = 20 \cdot 7 + 3$, $143 = 13 \cdot 11 + 0$. So 11 is a divisor.
List the primes p satisfying $11 \le p \le \sqrt{13}$: there are none. Thus 13 is prime and the prime factorization of 1001 is $1001 = 7^1 11^1 13^1$.

C2 (a) i.

$$\begin{array}{rcrcrcr} 94 &=& 47 &\cdot& 2 &+& 0 \\ 47 &=& 23 &\cdot& 2 &+& 1 \\ 23 &=& 11 &\cdot& 2 &+& 1 \\ 11 &=& 5 &\cdot& 2 &+& 1 \\ 5 &=& 2 &\cdot& 2 &+& 1 \\ 2 &=& 1 &\cdot& 2 &+& 0 \\ 1 &=& 0 &\cdot& 2 &+& 1 \end{array} \qquad (94)_{10} = (1011110)_2$$

ii.

$$\begin{array}{rcrcrcr} 231 &=& 115 &\cdot& 2 &+& 1 \\ 115 &=& 57 &\cdot& 2 &+& 1 \\ 57 &=& 28 &\cdot& 2 &+& 1 \\ 28 &=& 14 &\cdot& 2 &+& 0 \\ 14 &=& 7 &\cdot& 2 &+& 0 \\ 7 &=& 3 &\cdot& 2 &+& 1 \\ 3 &=& 1 &\cdot& 2 &+& 1 \\ 1 &=& 0 &\cdot& 2 &+& 1 \end{array} \qquad (231)_{10} = (11100111)_2$$

(b) i.

$$\begin{array}{rcrcrcr} 201 &=& 1 &\cdot& 111 &+& 90 \\ 111 &=& 1 &\cdot& 90 &+& 21 \\ 90 &=& 4 &\cdot& 21 &+& 6 \\ 21 &=& 3 &\cdot& 6 &+& 3 \\ 6 &=& 2 &\cdot& 3 &+& 0 \end{array} \qquad \gcd(111, 201) = 3$$

ii.

$$\begin{array}{rcrcrcr} 1331 &=& 1 &\cdot& 1001 &+& 330 \\ 1001 &=& 3 &\cdot& 330 &+& 11 \\ 330 &=& 30 &\cdot& 11 &+& 0 \end{array} \qquad \gcd(1001, 1331) = 11$$

C3 (a)

$$\begin{array}{rcrcrcr} 78 &=& 2 &\cdot& 35 &+& 8 \\ 35 &=& 4 &\cdot& 8 &+& 3 \\ 8 &=& 2 &\cdot& 3 &+& 2 \\ 3 &=& 1 &\cdot& 2 &+& 1 \\ 2 &=& 2 &\cdot& 1 &+& 0 \end{array} \qquad \begin{array}{rcrcccrcr} 1 &=& -1 &\cdot& 2 &+& 1 &\cdot& 3 \\ &=& -1 &\cdot& (8 - 2 \cdot 3) &+& 1 &\cdot& 3 \\ &=& 3 &\cdot& 3 &+& -1 &\cdot& 8 \\ &=& 3 &\cdot& (35 - 4 \cdot 8) &+& -1 &\cdot& 8 \\ &=& -13 &\cdot& 8 &+& 3 &\cdot& 35 \\ &=& -13 &\cdot& (78 - 2 \cdot 35) &+& 3 &\cdot& 35 \\ &=& 29 &\cdot& 35 &+& -13 &\cdot& 78 \end{array}$$

(b) $x = 29 \cdot 6 \textbf{ mod } 78 = 174 \textbf{ mod } 78 = (2 \cdot 78 + 18) \textbf{ mod } 78 = 18$

C4 (a)

i	a_i	x	*power*
		1	7
0	0	1	9
1	1	9	1
2	0	9	1
3	1	9	1
4	1	9	1

$7^{26} \bmod 20 = 9$

(b) 5^{601} **mod** $7 = 5^{100 \cdot 6+1}$ **mod** $7 = \left(5^6\right)^{100} \cdot 5^1$ **mod** $7 = 5^1$ **mod** $7 = 5$

C5 (a) The encryption function is $n \mapsto n^{1001}$ **mod** 10403.

(b) You need to know the prime factorization of n. The modulus n should factor as the product of two distinct primes $n = pq$. (In this case it does: $10403 = 101 \cdot 103$.)

(c) The number d is a multiplicative inverse of e modulo $(p-1)(q-1)$ which can be found using the extended Euclidean algorithm. (In this case, $(p-1)(q-1) = 100 \cdot 102 = 10200$ and $d = 2201$ is such an inverse.)

(d) The decryption function is $n \mapsto n^d$ **mod** 10403.

D1 (a)

n	$\frac{1}{1\cdot 2} + \frac{1}{2\cdot 3} + \cdots + \frac{1}{n(n+1)}$
1	$\frac{1}{1\cdot 2} = \frac{1}{2}$
2	$\frac{1}{1\cdot 2} + \frac{1}{2\cdot 3} = \frac{2}{3}$
3	$\frac{1}{1\cdot 2} + \frac{1}{2\cdot 3} + \frac{1}{3\cdot 4} = \frac{3}{4}$
4	$\frac{1}{1\cdot 2} + \frac{1}{2\cdot 3} + \frac{1}{3\cdot 4} + \frac{1}{4\cdot 5} = \frac{4}{5}$

Conjecture: $\forall n \in \mathbb{Z}^+, \dfrac{1}{1\cdot 2} + \dfrac{1}{2\cdot 3} + \cdots + \dfrac{1}{n(n+1)} = \dfrac{n}{n+1}$.

(b) **Basis Step**. The statement is true for $n = 1$. We verified this in part (a).

Inductive Step. Let $n \in \mathbb{Z}^+$ be arbitrary. Assume $\dfrac{1}{1\cdot 2} + \dfrac{1}{2\cdot 3} + \cdots + \dfrac{1}{n(n+1)} = \dfrac{n}{n+1}$. Then

$$\begin{aligned}
\frac{1}{1\cdot 2} + \frac{1}{2\cdot 3} + \cdots + \frac{1}{(n+1)((n+1)+1)} &= \frac{1}{1\cdot 2} + \frac{1}{2\cdot 3} + \cdots + \frac{1}{n(n+1)} + \frac{1}{(n+1)(n+2)} \\
&= \frac{n}{n+1} + \frac{1}{(n+1)(n+2)} = \frac{n(n+2)+1}{(n+1)(n+2)} \\
&= \frac{n^2+2n+1}{(n+1)(n+2)} = \frac{(n+1)^2}{(n+1)(n+2)} = \frac{n+1}{n+2} \\
&= \frac{n+1}{(n+1)+1}
\end{aligned}$$

D2 (a)

s	0	1	0	2	1	0	3	2	1	0	4	3	2	1	0
t	0	0	1	0	1	2	0	1	2	3	0	1	2	3	4
$3s+5t$	0	3	5	6	8	10	9	11	13	15	12	14	16	18	20

Conjecture: Postage n can be formed using 3-cent and 5-cent stamps if $n = 0, 3, 5, 6$ or $n \geq 8$.

(b) We will prove the conjecture for $n \geq 8$ using strong induction. (We verified the conjecture for $n = 0, 3, 5, 6$ in part (a).)

Basis Step. The statement is true for $n = 8, 9, 10$. We verified this in part (a).

Inductive Step. Let $n \geq 10$ be arbitrary. Assume the result is true for $8, \ldots, n$. Then $n \geq 10$ implies $n - 2 \geq 8$ so that there exist nonnegative integers s and t such that $n - 2 = 3s + 5t$. Then

$$n + 1 = (n-2) + 3 = 3s + 5t + 3 = 3(s+1) + 5t.$$

D3 (a)

$$\begin{aligned}
f(1) &= 0^2 + 0 + 1 &= 1 \\
f(2) &= 1^2 + 1 + 1 &= 3 \\
f(3) &= 3^2 + 3 + 1 &= 13 \\
f(4) &= 13^2 + 13 + 1 &= 183
\end{aligned}$$

(b) $a_0 = 0$ and $a_{n+1} = a_n + 6$ for each $n \in \mathbb{N}$

(c) S is the set of all multiples of 7: $7 \in S$, $0 = 7 - 7 \in S$, $-7 = 0 - 7 \in S$, $14 = 7 - (-7) \in S$, $-14 = -7 - 7 \in S$, $21 = 14 - (-7) \in S$, $-21 = -14 - 7 \in S$, ...