King Fahd University of Petroleum and Minerals
College of Computer Sciences and Engineering
Information and Computer Science Department

ICS 254: Discrete Structures II
Spring semester 2015-2016 (152)
Major Exam #1, Wednesday February 17, 2016
Time: **100** Minutes

Name: Sample Solution

ID#: ____________________

Instructions:
1. The exam consists of 7 pages, including this page, containing 6 questions.
2. Answer all questions. **Show all the steps.**
3. Make sure your answers are **clear** and **readable**.
4. The exam is closed book and closed notes. No calculators or any helping aides are allowed. Make sure you turn off your mobile phone and keep it in your pocket.
5. If there is no space on the front of the page, use the back of the page.

Question	Maximum Points	Earned Points
1	25	
2	10	
3	15	
4	20	
5	20	
6	10	
Total	**100**	

Q1: [25 points] Evaluate the following.

a) [3 points] $-23 \bmod 4$

$-23 = -6(4) + 1$ <3, ~~1~~ 7>

$\therefore -23 \pmod 4 = 1$

b) [6 points] $(32^3 \bmod 13)^2 \bmod 11$

$32 \bmod 13 = 6$ — 2

$\therefore (32^3 \pmod{13}) \equiv 6^3 \pmod{13} \equiv 10(6) \pmod{13}$

$\equiv 60 \pmod{13} \equiv 8$ — 2

$8^2 \pmod{11} \equiv (-3)^2 \pmod{11}$

$\equiv 9 \pmod{11}$ — 2

c) [6 points] $(20CBA)_{16} = ($ 0406272 $)_8$

2 0 C B A (+3)

0010 0000 1100 1011 1010

000 100 000 110 010 111 010 (+3)

0 4 0 6 2 7 2

d) [10 points] $(20CBA)_{16} \times (2D)_{16}$

1010	1011	1100	1101	1110	1111
A	B	C	D	E	F
10	11	12	13	14	15

```
  20CBA
     2D  x
 ------
 1AA572   -- 4
 419740   -- 4
 ------
 5C3CB2   -- 2
```

+5 : Multiplication

+5 : Addition

OR [if transformed into Binary]

8F + 8 = 97

9C + 9 = A5

$8 \times 16 = 128$

13 × 11 = 143

16 | 130 = 8 … 2

16 | 143 = 8 … F

16 | 156 = 9 … C

Q2: [10 points] Using the modular exponentiation algorithm, find 13^{1057} mod 9

	x	P
	1	13 mod 9 = 4
1	4	7
0		4
0		7
0		4
0		7
1	1	4
0		7
0		4
0		7
0		4
1	4	

1	2	1057
0	2	528
0	2	264
0	2	132
0	2	66
1	2	33
0	2	16
0	2	8
0	2	4
0	2	2
1	2	1
		0

+3

$13^{1057} \equiv 4 \pmod 9$

+1

~~<7, 6, 5, 3>~~

<6, 5, 3>

Q3: [15 points]

a) [5 points] Find the prime factorization of 10!

$$10! = 10 \cdot 3^2 \cdot 2^3 \cdot 7 \cdot 6 \cdot 5 \cdot 2^2 \cdot 3 \cdot 2$$
$$= 2 \cdot 5 \cdot 3^2 \cdot 2^3 \cdot 7 \cdot 2 \cdot 3 \cdot 5 \cdot 2^2 \cdot 3 \cdot 2$$
$$= 2^8 \cdot 3^4 \cdot 5^2 \cdot 7$$

+2 +1 +1 +1

b) [10 points] Show that if a positive integer is divisible by 3, then the sum of its digits is divisible by 3.

Let $k = (a_n a_{n-1} a_{n-2} \cdots a_1 a_0)$.

We have $k \equiv 0 \pmod 3$. +3

$$a_n a_{n-1} a_{n-2} \cdots a_1 a_0 = a_0 + a_1(10) + a_2(10^2) + \cdots + a_{n-1}(10^{n-1}) + a_n 10^n.$$

$$= a_0 + a_1(1) + a_2(1^2) + \cdots + a_n(1)^n \pmod 3$$

[since $10 \equiv 1 \pmod 3$]

~~<1, 6, 2, 4>~~

<7, 6, 3, 1>

$$= a_0 + a_1 + \cdots + a_n \pmod 3$$
$$= 0 \pmod 3 \text{ [Given]}$$

$$\therefore \sum_{j=0}^{n} a_j = 0 \pmod 3$$

$$\therefore 3 \mid \sum_{j=0}^{n} a_j.$$

Q4: [20 points]

a) [10 points] Find gcd(4727, 3973) using the Euclidean algorithm.

$4727 = 3973 + 754$ — 1

$3973 = 5(754) + 203$ — 2

$754 = 3(203) + 145$ — 2

$203 = 145 + 58$ — 1

$145 = 2(58) + 29$ — 2

$58 = 2(29) + 0$ — 1

$\therefore \gcd(4727, 3973) = 29$ — +1

b) [10 points] Express the greatest common divisor of 4727 and 3973 as a linear combination of these two numbers.

$$
\begin{aligned}
29 &= 145 - 2(58) \\
&= 145 - 2[203 - 145] \\
&= 3(145) - 2(203) \\
&= 3[754 - 3(203)] - 2(203) \\
&= 3(754) - 11(203) \\
&= 3(754) - 11(3973 - 5(754)) \\
&= 58(754) - 11(3973) \\
&= 58[4727 - 3973] - 11(3973) \\
&= 58(4727) - 69(3973)
\end{aligned}
$$

<10, 8, 5, 1>

<10, 8, 7, 5, 1>

-3 if a is wrong.

Q5: [20 points] Solve the following system of linear congruences

$$3x \equiv 5 \pmod 7$$
$$2x \equiv 7 \pmod{11}$$
$$7x \equiv 1 \pmod{10}$$

First, Let us write the equations in the form $x \equiv y \pmod z$.

$5 \cdot 3x \equiv 5 \cdot 5 \pmod 7 \Rightarrow$ $\boxed{x \equiv 4 \pmod 7}$

$6 \cdot 2x \equiv 6 \cdot 7 \pmod{11} \Rightarrow$ $\boxed{x \equiv 9 \pmod{11}}$

$3 \times 7x \equiv 3 \times 1 \pmod{10} \Rightarrow$ $\boxed{x \equiv 3 \pmod{10}}$

+5

We can apply the chinese remainder theorem on the congrunces.

Now, we use the back substitution method.

$x \equiv 4 \pmod 7 \Rightarrow x = 7k + 4$ +3

$x \equiv 9 \pmod{11} \Rightarrow (7k+4) \equiv 9 \pmod{11}$ +3

$\Leftrightarrow 7k \equiv 5 \pmod{11}$

$\Leftrightarrow_{8\times} k \equiv 8 \cdot 5 \pmod{11} \equiv 7 \pmod{11}$

$\therefore k = 11t + 7$ +3

Now $x = 7k + 4 = 7(11t+7) + 4$

$= 77t + 53$. +2

$\therefore (77t + 53) \equiv 3 \bmod 10$

$7t + 3 \equiv 3 \bmod 10$

$7t \equiv 0 \bmod 10$ +2

$t \equiv 0$

$\therefore t = 10w$

$\therefore x = 77(10w) + 53$ +2

$= 770w + 53$

$= 53.$

Q5: [20 points] Solve the following system of linear congruences

$$3x \equiv 5 \pmod{7}$$
$$2x \equiv 7 \pmod{11}$$
$$7x \equiv 1 \pmod{10}$$

$x \equiv 25 \bmod 7 = 4 \bmod 7$

$x \equiv 42 \bmod 11 = 9 \bmod 11$ +5

$x \equiv 3 \bmod 10 = 3 \bmod 10$

$M_1 = 110$

$M_2 = 70$ +3

$M_3 = 77$

$110 y_1 = 1 \bmod 7$ $\quad y_1 = 3 \bmod 7$

$70 y_2 = 1 \bmod 11$ $\quad y_2 = 3 \bmod 11$ +6

$77 y_3 = 1 \bmod 10$ $\quad y_3 = 3 \bmod 10$

$x = 110 \cdot 3 \cdot 4 + 70 \cdot 3 \cdot 9 + 77 \cdot 3 \cdot 3$

$= 440(3) + 630(3) + 231(3)$

$= 1320 + 1890 + 693$ +6

$= 3903 \bmod 770$

$= \boxed{53}$

X

$x \equiv 4 \bmod 7$

$x = 7k + 4$

$7k + 4 = 9 \bmod 11$

$7k = 5 \bmod 11$

$k \equiv 40 \bmod 11 \equiv 7 \bmod 11$

$k = 7j + 11$

$7j + 11 \equiv 3 \bmod 10$

$7j \equiv -8 \bmod 10 \equiv 2 \bmod 10$

$j \equiv 6 \bmod 10$

$k = 7(6) + 11 = 53$

$x = 7(53) + 4 = 366$

$7\overline{)12}$ $\quad 7\overline{)16}$ $\quad 12$

$7\overline{)89}$, 63

$7\overline{)366}$: 52; 35, 16, 14, 2

$11\overline{)42}$: 33, 9 $\quad 7\overline{)28}$: 21, 4 $\quad 11\overline{)42}$: 33, 9

$7\overline{)110}$: 1; 7, 40

$7\overline{)220}$: 31; 21, 10

$7\overline{)330}$: 47; 28, 50, 49, 1

$7\overline{)330}$: 47; 28, 50, 49

$11\overline{)210}$: 18; 11, 100, 88

$11\overline{)280}$: 25; 22, 60

$11\overline{)350}$: 31; 33, 20, 11

$11\overline{)420}$: 3; 33, 90

1320
1890
693
3903

$770\overline{)3903}$: 5; 3850, 53

$7\overline{)53}$: 7; 49, 4

Q6: [10 points] Using Fermat's little theorem, compute 13^{1057} mod 23

$$\begin{array}{r} 48 \\ 22\,\big)\,1057 \\ 88 \\ \hline 177 \\ 176 \\ \hline 1 \end{array}$$

$\therefore \; 1057 = (48)(22) + 1$

+3

$\therefore \; 13^{1057} \pmod{23} = 13^{(48)(22)+1} \pmod{23}$ +1

$= \left(13^{22}\right)^{48} \cdot 13 \pmod{23}$ +2

$= 1^{48} \cdot 13 \pmod{23}$ +3

$= 13 \pmod{23}$ +1