CS 70 First Midterm 3 Mar 2011

NAME (1 pt): ______________________________

SID (1 pt): ______________________________

TA (1 pt): ______________________________

Name of Neighbor to your left (1 pt): ______________________________

Name of Neighbor to your right (1 pt): ______________________________

Instructions: This is a closed book, closed calculator, closed computer, closed network, open brain exam, but you are permitted a 1 page, double-sided set of notes, large enough to read without a magnifying glass.

You get one point each for filling in the 5 lines at the top of this page. Each other question is worth 20 points.

Write all your answers on this exam. If you need scratch paper, ask for it, write your name on each sheet, and attach it when you turn it in (we have a stapler).

1	
2	
3	
4	
5	
6	
Total	

Answers

Question 1 (20 points) Logic.

For each of the following propositions, circle either *True* if it is always true, *False* if it is always false, or *Depends* if its value could be either true or false, depending on more information. For example, if we are given no information about propositions p and q, then for $p \vee q$ the right answer would be *Depends.* You do not have to justify your answer. **Each part is worth 5 points, but we will subtract 2 points for the wrong answer, so guessing may not help.** We let $\mathbb{N} = \{0, 1, 2, ...\}$ denote the natural numbers, $\mathbb{Q}$ denote the rational numbers, and $p \otimes q$ denote $\neg(p \vee q)$.

1.1 (5 points). *True False Depends.* Here x, y and z denote propositions, each of which could be True or False:

$$((x \otimes y) \vee \neg z) \rightarrow (z \rightarrow \neg y)$$

Answer: *True*, because

$$\begin{aligned}
((x \otimes y) \vee \neg z) \rightarrow (z \rightarrow \neg y) &\Longleftrightarrow \\
(\neg(x \vee y) \vee \neg z) \rightarrow (z \rightarrow \neg y) &\Longleftrightarrow \\
(\neg(x \vee y) \vee \neg z) \rightarrow (\neg z \vee \neg y) &\Longleftrightarrow \\
\neg(\neg(x \vee y) \vee \neg z) \vee (\neg z \vee \neg y) &\Longleftrightarrow \\
((x \vee y) \wedge z) \vee (\neg z \vee \neg y) &\Longleftrightarrow \\
(x \wedge z) \vee (y \wedge z) \vee (\neg z \vee \neg y) &\Longleftrightarrow \\
(x \wedge z) \vee (y \wedge z) \vee \neg(z \wedge y) &\Longleftrightarrow \\
(x \wedge z) \vee s \vee \neg s \quad \text{where } s = (z \wedge y) &\Longleftrightarrow \\
(x \wedge z) \vee True &\Longleftrightarrow True
\end{aligned}$$

1.2 (5 points). *True False Depends.*

$$\forall a \in \mathbb{N} \ \ \exists b \in \mathbb{Q} \ \ (a = b^2)$$

Answer: *False*: This statement says that all natural numbers have rational square roots, but we know, for example, that if $a = 2$ then $b = 2^{1/2}$ is not rational.

1.3 (5 points). *True False Depends.* Here $R(k)$ and $S(k)$ are propositions that depend on the natural number k.

$$[\forall k \in \mathbb{N} \ \ (\neg R(k) \rightarrow S(k))] \vee [\exists j \in \mathbb{N} \ \ (\neg S(j) \wedge \neg R(j))]$$

Answer: *True*: This proposition of the form $p \vee q$; negating p we get

$$\neg p \Longleftrightarrow \neg[\forall k \in \mathbb{N} \ \ (\neg R(k) \rightarrow S(k))] \Longleftrightarrow$$

$$[\exists k \in \mathbb{N} \ \ \neg(\neg R(k) \rightarrow S(k))] \Longleftrightarrow$$

$$[\exists k \in \mathbb{N} \ \ \neg(\neg\neg R(k) \vee S(k))] \Longleftrightarrow$$

$$[\exists k \in \mathbb{N} \ \ \neg(R(k) \vee S(k))] \Longleftrightarrow$$

$$[\exists k \in \mathbb{N} \ \ (\neg R(k) \wedge \neg S(k))] \Longleftrightarrow q$$

so the whole proposition is of the form $p \vee \neg p$ which is true.

1.4 (5 points). *True False Depends.*

$$\neg[(p \vee q \vee r) \wedge (\neg q \vee p \vee \neg r) \wedge (\neg r \vee p \vee q) \wedge (\neg q \vee r \vee p)]$$

Answer: *Depends*: Simplifying the proposition gives us

$$\begin{aligned}
\neg[(p \vee q \vee r) \wedge (\neg q \vee p \vee \neg r) \wedge (\neg r \vee p \vee q) \wedge (\neg q \vee r \vee p)] &\iff \\
\neg(p \vee q \vee r) \vee \neg(\neg q \vee p \vee \neg r) \vee \neg(\neg r \vee p \vee q) \vee \neg(\neg q \vee r \vee p) &\iff \\
(\neg p \wedge \neg q \wedge \neg r) \vee (q \wedge \neg p \wedge r) \vee (r \wedge \neg p \wedge \neg q) \vee (q \wedge \neg r \wedge \neg p) &\iff \\
\neg p \wedge [(\neg q \wedge \neg r) \vee (q \wedge r) \vee (r \wedge \neg q) \vee (q \wedge \neg r)] &\iff \\
\neg p \wedge True &\iff \neg p
\end{aligned}$$

so it depends on p.

Question 1 (20 points) Logic.

For each of the following propositions, circle either *True* if it is always true, *False* if it is always false, or *Maybe* if its value could be either true or false, depending on more information. For example, if we are given no information about propositions x and y, then for $x \wedge y$ the right answer would be *Maybe*. You do not have to justify your answer. **Each part is worth 5 points, but we will subtract 2 points for the wrong answer, so guessing may not help.** We let $\mathbb{N} = \{0, 1, 2, ...\}$ denote the natural numbers, $\mathbb{Q}$ denote the rational numbers, and $p \uparrow q$ denote $\neg(p \vee q)$.

1.1 (5 points). *True False Maybe.*

$$\forall r \in \mathbb{N} \ \exists s \in \mathbb{Q} \ \ (s^2 = r)$$

Answer: *False*: This statement says that all natural numbers have rational square roots, but we know, for example, that if $r = 2$ then $s = 2^{1/2}$ is not rational.

1.2 (5 points). *True False Maybe.* Here $T(i)$ and $V(i)$ are propositions that depend on the natural number i.

$$[\forall i \in \mathbb{N} \ \ (\neg T(i) \rightarrow V(i))] \vee [\exists m \in \mathbb{N} \ \ (\neg V(m) \wedge \neg T(m))]$$

Answer: *True*: This proposition of the form $p \vee q$; negating p we get

$$\neg p \Longleftrightarrow \neg[\forall i \in \mathbb{N} \ \ (\neg T(i) \rightarrow V(i))] \Longleftrightarrow$$

$$[\exists i \in \mathbb{N} \ \ \neg(\neg T(i) \rightarrow V(i))] \Longleftrightarrow$$

$$[\exists i \in \mathbb{N} \ \ \neg(\neg\neg T(i) \vee V(i))] \Longleftrightarrow$$

$$[\exists i \in \mathbb{N} \ \ \neg(T(i) \vee V(i))] \Longleftrightarrow$$

$$[\exists i \in \mathbb{N} \ \ (\neg T(i) \wedge \neg V(i))] \Longleftrightarrow q$$

so the whole proposition is of the form $p \vee \neg p$ which is true.

1.3 (5 points). *True False Maybe.*

$$\neg[(\neg c \vee d \vee \neg b) \wedge (\neg c \vee \neg b \vee \neg d) \wedge (\neg d \vee \neg b \vee c) \wedge (\neg b \vee c \vee d)]$$

Answer: *Maybe*: Simplifying the proposition gives us

$$\begin{aligned}
\neg[(\neg b \vee c \vee d) \wedge (\neg c \vee \neg b \vee \neg d) \wedge (\neg d \vee \neg b \vee c) \wedge (\neg c \vee d \vee \neg b)] &\Longleftrightarrow \\
\neg(\neg b \vee c \vee d) \vee \neg(\neg c \vee \neg b \vee \neg d) \vee \neg(\neg d \vee \neg b \vee c) \vee \neg(\neg c \vee d \vee \neg b) &\Longleftrightarrow \\
(\neg\neg b \wedge \neg c \wedge \neg d) \vee (c \wedge \neg\neg b \wedge d) \vee (d \wedge \neg\neg b \wedge \neg c) \vee (c \wedge \neg d \wedge \neg\neg b) &\Longleftrightarrow \\
\neg\neg b \wedge [(\neg c \wedge \neg d) \vee (c \wedge d) \vee (d \wedge \neg c) \vee (c \wedge \neg d)] &\Longleftrightarrow \\
b \wedge True &\Longleftrightarrow b
\end{aligned}$$

so it depends on b.

1.4 (5 points). *True False Maybe.* Here r, s and t denote propositions, each of which could be True or False:

$$(\neg t \vee (r \uparrow s)) \rightarrow (t \rightarrow \neg s)$$

Answer: *True*, because

$$\begin{aligned}
((r \uparrow s) \vee \neg t) \rightarrow (t \rightarrow \neg s) &\iff \\
(\neg(r \vee s) \vee \neg t) \rightarrow (t \rightarrow \neg s) &\iff \\
(\neg(r \vee s) \vee \neg t) \rightarrow (\neg t \vee \neg s) &\iff \\
\neg(\neg(r \vee s) \vee \neg t) \vee (\neg t \vee \neg s) &\iff \\
((r \vee s) \wedge t) \vee (\neg t \vee \neg s) &\iff \\
(r \wedge t) \vee (s \wedge t) \vee (\neg t \vee \neg s) &\iff \\
(r \wedge t) \vee (s \wedge t) \vee \neg(t \wedge s) &\iff \\
(r \wedge t) \vee w \vee \neg w \quad \text{where } w = (t \wedge s) &\iff \\
(r \wedge t) \vee True \iff True
\end{aligned}$$

Question 2 (20 points) Induction.

Prove, using induction, that the following proposition is true for all positive integers n: $P(n) =$ "$\sum_{i=1}^{n} i^3 = (\sum_{i=1}^{n} i)^2$."

Question 2.1 (4 points): State and prove the base case for the induction.

Answer:

$$\sum_{i=1}^{1} i^3 = 1^3 = 1$$
$$= 1^2 = \left(\sum_{i=1}^{1} i\right)^2.$$

Question 2.2 (16 points): State and prove the inductive step, and thus complete the proof. **Hint:** First find (and prove) a formula for $\sum_{i=1}^{n} i$, which we proved in two different ways in lecture.

Answer:

First we show that $s = \sum_{i=1}^{n} i = \frac{n(n+1)}{2}$. One proof:

$$\begin{aligned} s &= 1 + 2 + \cdots + (n-1) + n \\ +s &= n + (n-1) + \cdots + 2 + 1 \\ \hline 2s &= (n+1) + (n+1) + \cdots + (n+1) + (n+1) \\ s &= \frac{n(n+1)}{2} \end{aligned}$$

For an inductive proof, see Note 3. Now we rewrite our proposition as $P(n) =$"$\sum_{i=1}^{n} i^3 = \left(\frac{n(n+1)}{2}\right)^2$."

Assume $P(n)$ is true:

$$\begin{aligned} P(n) &\Rightarrow \\ \sum_{i=1}^{n+1} i^3 &= \sum_{i=1}^{n} i^3 + (n+1)^3 \\ &= \left(\frac{n(n+1)}{2}\right)^2 + (n+1)^3 \\ &= (n+1)^2 \left[\frac{n^2}{4} + (n+1)\right] \\ &= (n+1)^2 \frac{n^2+4n+4}{4} \\ &= \frac{(n+1)^2(n+2)^2}{4} \\ &= \left(\frac{(n+1)((n+1)+1)}{2}\right)^2 \\ &\Rightarrow P(n+1) \end{aligned}$$

thus completing the proof.

Question 2 (20 points) Induction.

Prove, using induction, that the following equality is true for all positive integers m: $\left[\sum_{j=1}^{m} j\right]^2 = \sum_{j=1}^{m} j^3$.

Question 2.1 (4 points): State and prove the base case for the induction.

Answer:

$$\begin{aligned}\sum_{j=1}^{1} j^3 &= 1^3 = 1 \\ &= 1^2 = \left(\sum_{j=1}^{1} j\right)^2.\end{aligned}$$

Question 2.2 (16 points): State and prove the inductive step, and thus complete the proof. **Hint:** First find (and prove) a formula for $\sum_{j=1}^{m} j$, which we proved in two different ways in lecture.

Answer:

First we show that $s = \sum_{j=1}^{m} j = \frac{m(m+1)}{2}$. One proof:

$$\begin{aligned} s &= 1 + 2 + \cdots + (m-1) + m \\ +s &= m + (m-1) + \cdots + 2 + 1 \\ \hline \\ 2s &= (m+1) + (m+1) + \cdots + (m+1) + (m+1) \\ s &= \frac{m(m+1)}{2} \end{aligned}$$

For an inductive proof, see Note 3. Now we rewrite our proposition as $P(m) =$"$\sum_{j=1}^{m} j^3 = \left(\frac{m(m+1)}{2}\right)^2$."

Assume $P(m)$ is true:

$$\begin{aligned} P(m) &\Rightarrow \\ \sum_{j=1}^{m+1} j^3 &= \sum_{j=1}^{m} j^3 + (m+1)^3 \\ &= \left(\frac{m(m+1)}{2}\right)^2 + (m+1)^3 \\ &= (m+1)^2 \left[\frac{m^2}{4} + (m+1)\right] \\ &= (m+1)^2 \frac{m^2+4m+4}{4} \\ &= \frac{(m+1)^2 (m+2)^2}{4} \\ &= \left(\frac{(m+1)((m+1)+1)}{2}\right)^2 \\ &\Rightarrow P(m+1) \end{aligned}$$

thus completing the proof.

Question 3 (20 points) Stable Marriage.

1. (10 points) Consider an instance of the Stable Marriage problem in which the men are $\{1, 2, 3, 4\}$, the women are $\{A, B, C, D\}$, and the preference lists (from most preferred on the left to least preferred on the right) are

Men (1-4)					Women (A-D)				
1:	A	B	D	C	A:	2	3	4	1
2:	C	B	D	A	B:	1	4	2	3
3:	D	C	B	A	C:	1	4	2	3
4:	D	C	A	B	D:	1	2	3	4

Find a female-optimal pairing. Write your answer in the following box: (1 ,) (2 ,) (3 ,) (4 ,)

Who are the persons who have been proposed to by the end of round 2, and to whom have they said 'maybe' in round 2? Write your answer in the following box, as a list of pairs: (person proposed to, proposer). For example, (x,y) would mean y proposed to x in round 2.

[ ]

Answer:

(1,B) (2,D) (3,A) (4,C)

[(1,B), (2,D), (3, no one yet), (4,C)]

2. (10 points) Given n men and n women, for any $n \geq 2$, what is the minimum number of stable pairings that must exist for any sets of preferences? Justify your answer with a specific example attaining the minimum.

Answer: One pairing: We know that the Stable Marriage algorithm always terminates with one stable pairing, so we need to show that there is a set of preferences for which there is only one stable pairing. Let the Men be $M_1, ..., M_n$ and the Women be $W_1, ..., W_n$. Suppose that for every $1 \leq i \leq n$, M_i's top-ranked person is W_i, and W_i's top-ranked person is M_i. Then the pairing that matches up all (M_i, W_i) is the only stable pairing, because if M_i and W_i are not paired, they will be a rogue couple.

Question 3 (20 points) Stable Marriage.

1. (10 points) Consider an instance of the Stable Marriage problem in which the men are $\{1, 2, 3, 4\}$, the women are $\{W, X, Y, Z\}$, and the preference lists (from most preferred on the left to least preferred on the right) are

Men (1-4)					Women (W-Z)				
1:	Y	X	Z	W	W:	4	3	2	1
2:	Z	X	Y	W	X:	4	2	1	3
3:	W	Y	X	Z	Y:	3	4	1	2
4:	Z	W	Y	X	Z:	2	3	1	4

Find a female-optimal pairing. Write your answer in the following box: (1 ,) (2 ,) (3 ,) (4 ,)

Who are the persons who have been proposed to by the end of round 2, and to whom have they said 'maybe' in round 2? Write your answer in the following box, as a list of pairs: (person proposed to, proposer). For example, (x,y) would mean y proposed to x in round 2.

[ ]

Answer:

(1,X) (2,Z) (3,Y) (4,W)

[(1,no one yet), (2,Z), (3, Y), (4,W)]

2. (10 points) Given m men and m women, for any $m \geq 2$, what is the minimum number of stable pairings that must exist for any sets of preferences? Justify your answer with a specific example attaining the minimum.

Answer: One pairing: We know that the Stable Marriage algorithm always terminates with one stable pairing, so we need to show that there is a set of preferences for which there is only one stable pairing. Let the Men be $M_1, ..., M_m$ and the Women be $W_1, ..., W_m$. Suppose that for every $1 \leq i \leq m$, M_i's top-ranked person is W_i, and W_i's top-ranked person is M_i. Then the pairing that matches up all (M_i, W_i) is the only stable pairing, because if M_i and W_i are not paired, they will be a rogue couple.

Question 4 (20 points) Modular Arithmetic.

Question 4.1 (7 points): Use the extended Euclidean algorithm to find $gcd(7, 47)$ and integers x and y such that $7 \cdot x + 47 \cdot y = gcd(7, 47)$. Show the intermediate results of the algorithm. Fill in your answers in the boxes below:

$\boxed{gcd(7, 47) = \qquad}$ $\boxed{x = \qquad}$ $\boxed{y = \qquad}$

Answer: e-gcd(47,7)
calls e-gcd(7,5)
calls e-gcd(5,2)
calls e-gcd(2,1)
calls e-gcd(1,0)
returns 1 = 1*1 + 0*0
returns 1 = 2*0 + 1*1
returns 1 = 5*1 + 2*(-2)
returns 1 = 7*(-2) + 5*3
returns 1 = 47*3 + 7*(-20)
so $x = -20$ and $y = 3$ and $gcd(7, 47) = 1$.

Question 4.2 (3 points): Solve $47 \cdot z \equiv 4 \mod 7$. Show your work. Fill in your answer in the box below:

$\boxed{z = \qquad}$

Answer: Multiply both sides of the congruence by the multiplicative inverse of 47 modulo 7, i.e. 3, to get $3 \cdot 47z \equiv 1 \cdot z \equiv z \equiv 3 \cdot 4 \equiv 5 \mod 7$.

Question 4.3 (10 points): How many distinct solutions of $3^{3^{3^{3^{3}}}} \cdot z + 43 \equiv 2^{2^{2^{2^{2}}}} \mod 21$ are there, modulo 21? Justify your answer. You do not need to find solutions explicitly, just count them. Fill in your answer in the box below:

$\boxed{\#\text{solutions} = \qquad}$

Answer: First note that $3^{3^{3^{3^{3}}}}$ = 3ˆ(3ˆ(3ˆ(3ˆ3))), not (((3ˆ3)ˆ3)ˆ3)ˆ3 = 3^{81}; the order of parentheses is important. The gcd of $3^{3^{3^{3^{3}}}}$ and 21 is 3. So by the extended Euclidean algorithm we can choose z and y to make $3^{3^{3^{3^{3}}}} \cdot z + 21 \cdot y$ equal to any integer multiple of 3, and only integer multiples of 3. So the question is whether $2^{2^{2^{2^{2}}}} - 43$ is an integer multiple of 3: We confirm this by computing $2^{2^{2^{2^{2}}}} - 43 \equiv (-1)^{2^{2^{2^{2}}}} - 1 \equiv (-1)^{\text{an even number}} - 1 \equiv 1 - 1 \equiv 0 \mod 3$. So there is at least one solution z. Furthermore, if z is a solution, so is $z + 7k$ for any integer k, since $3^{3^{3^{3^{3}}}} \cdot (z + 7k) \equiv 3^{3^{3^{3^{3}}}} \cdot z \mod 21$ for any k. Thus there are at least 3 distinct solutions, for $k = 0, 1, 2$. These are in fact all the solutions, because if z_1 and z_2 are solutions, then $3^{3^{3^{3^{3}}}} (z_1 - z_2) \equiv 0 \mod 21$, so $z_1 \equiv z_2 \mod 7$.

Question 4 (20 points) Modular Arithmetic.

Question 4.1 (7 points): Use the extended Euclidean algorithm to find $gcd(11, 53)$ and integers x and y such that $11 \cdot x + 53 \cdot y = gcd(11, 53)$. Show the intermediate results of the algorithm. Fill in your answers in the boxes below:

$\boxed{gcd(11, 53) = \quad}$ $\boxed{x = \quad}$ $\boxed{y = \quad}$

Answer: e-gcd(53,11)
calls e-gcd(11,9)
calls e-gcd(9,2)
calls e-gcd(2,1)
calls e-gcd(1,0)
returns 1 = 1*1 + 0*0
returns 1 = 2*0 + 1*1
returns 1 = 9*1 + 2*(-4)
returns 1 = 11*(-4) + 9*5
returns 1 = 53*5 + 11*(-24)
so $x = -24$ and $y = 5$ and $gcd(11, 53) = 1$.

Question 4.2 (3 points): Solve $53 \cdot a \equiv 3 \pmod{11}$. Show your work. Fill in your answer in the box below:

$\boxed{a = \quad}$

Answer: Multiply both sides of the congruence by the multiplicative inverse of 53 modulo 11, i.e. 5, to get $5 \cdot 53a \equiv 1 \cdot a \equiv a \equiv 5 \cdot 3 \equiv 4 \pmod{11}$.

Question 4.3 (10 points): How many distinct solutions of $5^{5^{5^{5^5}}} \cdot r + 16 \equiv 4^{4^{4^4}} \pmod{35}$ are there, modulo 35? Justify your answer. You do not need to find solutions explicitly, just count them. Fill in your answer in the box below:

$\boxed{\#\text{solutions} = \quad}$

Answer: First note that $3^{3^{3^{3^3}}}$ = 3ˆ(3ˆ(3ˆ(3ˆ3))), not (((3ˆ3)ˆ3)ˆ3)ˆ3 = 3^{81}; the order of parentheses is important. The gcd of $5^{5^{5^{5^5}}}$ and 35 is 5. So by the extended Euclidean algorithm we can choose r and y to make $5^{5^{5^{5^5}}} \cdot r + 35 \cdot y$ equal to any integer multiple of 5, and only integer multiples of 5. So the question is whether $4^{4^{4^4}} - 16$ is an integer multiple of 5: We confirm this by computing $4^{4^{4^4}} - 16 \equiv (-1)^{4^{4^4}} - 1 \equiv (-1)^{\text{an even number}} - 1 \equiv 1 - 1 \equiv 0 \pmod{5}$. So there is at least one solution r. Furthermore, if r is a solution, so is $r + 7k$ for any integer k, since $5^{5^{5^{5^5}}} \cdot (r + 7k) \equiv 5^{5^{5^{5^5}}} \cdot r \pmod{35}$ for any k. Thus there are at least 5 distinct solutions, for $k = 0, 1, 2, 3, 4$. These are in fact all the solutions, because if r_1 and r_2 are solutions, then $5^{5^{5^{5^5}}}(r_1 - r_2) \equiv 0 \pmod{35}$, so $r_1 \equiv r_2 \pmod{7}$.

Question 5 (20 points) RSA.

5.1 (10 points). Alice wants to receive an encrypted message using RSA from Bob, so she chooses $p = 11$ and $q = 3$.

(a) What values of e can Alice use for the public key?
Answer: e must be mutually prime with $(p-1)(q-1) = 20$ therefore e cannot have a factor of 2 or 5 in it. Valid values for e are $1, 3, 7, 9, 11, 13, 17, 19 \bmod 20$.

(b) Alice chooses $e = 7$. Find d.
Answer:

$$ed \equiv 1 \bmod 20$$

Without using extended gcd we can see that $d = 3$ is the inverse of 7 modulo 20 since $3 \cdot 7 = 21$.

5.2 (5 points). Bob sends Alice his public key $(n = 65, e = 11)$, so Alice can send the message $m = 8$. What encrypted value $E(m)$ will Alice send back to Bob?

Answer:

$$E(m) = m^e \bmod n = 8^{11} \bmod 65$$

$$\begin{aligned}
8^1 &\equiv 8 \bmod 65 \\
8^2 &\equiv 64 \bmod 65 \\
&\equiv -1 \bmod 65 \\
8^4 &\equiv (-1)^2 \bmod 65 \\
&\equiv 1 \bmod 65 \\
8^8 &\equiv 1 \bmod 65 \\
8^{11} &\equiv 8^8 \cdot 8^2 \cdot 8^1 \bmod 65 \\
&\equiv 1 \cdot -1 \cdot 8 \bmod 65 \\
&\equiv -8 \bmod 65 \\
&\equiv 57 \bmod 65
\end{aligned}$$

Alice sends $E(m) = 57$

5.3 (5 points). Alice has a database of private information and she would like all the values b_i multiplied by x, but she doesn't have the computing resources. Dave has a cluster of computers that Alice would like to use without revealing any of the data to Dave. Alice sends Dave her public key (n, e), the values in the database encrypted with her public key $E(b_i)$, and the number encrypted with her public key $E(x)$. How can Dave calculate the encryption of database values multiplied by x, $E(b_i x)$, without Alice's private key?

Answer: Dave can multiply $E(x)$ by $E(b_i)$ modulo n to get $E(b_i x)$.

$$\begin{aligned}
E(b_i x) &= (b_i x)^e \bmod n \\
&\equiv (b_i)^e (x)^e \bmod n \\
&\equiv E(b_i) E(x) \bmod n
\end{aligned}$$

Question 5 (20 points) RSA.

5.1 (10 points). Alice wants to receive an encrypted message using RSA from Bob, so she chooses $p = 7$ and $q = 5$.

(a) What values of e can Alice use for the public key?
Answer: e must be mutually prime with $(p-1)(q-1) = 24$ therefore e cannot have a factor of 2 or 3 in it. Valid values for e are $1, 5, 7, 11, 13, 17, 19, 23 \bmod 24$

(b) Alice chooses $e = 5$. Find d.
Answer:

$$ed \equiv 1 \bmod 24$$

Without using extended gcd we can see that $d = 5$ is the inverse of 5 modulo 24 since $5 \cdot 5 = 25$.

5.2 (5 points). Bob sends Alice his public key $(n = 82, e = 11)$ so Alice can send the message $m = 9$. What encrypted value $E(m)$ will Alice send back to Bob?

Answer:

$$E(m) = m^e \bmod n = 9^{11} \bmod 82$$

$$\begin{aligned}
9^1 &\equiv 9 \bmod 82 \\
9^2 &\equiv 81 \bmod 82 \\
&\equiv -1 \bmod 81 \\
9^4 &\equiv (-1)^2 \bmod 82 \\
&\equiv 1 \bmod 82 \\
9^8 &\equiv 1 \bmod 82 \\
9^{11} &\equiv 9^8 \cdot 9^2 \cdot 9^1 \bmod 82 \\
&\equiv 1 \cdot -1 \cdot 9 \bmod 82 \\
&\equiv -9 \bmod 82 \\
&\equiv 73 \bmod 82
\end{aligned}$$

Alice sends $E(m) = 73$

5.3 (5 points). Alice has a database of private information and she would like all the values p_i multiplied by z, but she doesn't have the computing resources. Dave has a cluster of computers that Alice would like to use without revealing any of the data to Dave. Alice sends Dave her public key (n, e), the values in the database encrypted with her public key $E(p_i)$, and the number encrypted with her public key $E(z)$. How can Dave calculate the encryption of database values multiplied by z, $E(p_i z)$, without Alice's private key?

Answer: Dave can multiply $E(z)$ by $E(p_i)$ modulo n to get $E(p_i z)$.

$$\begin{aligned}
E(p_i z) &= (p_i z)^e \bmod n \\
&\equiv (p_i)^e (z)^e \bmod n \\
&\equiv E(p_i) E(z) \bmod n
\end{aligned}$$

Question 6 (20 points) Polynomials and Error Correcting Codes.

6.1 (6 points). In a programming assignment, you are asked to write a program that computes

$$z = 2560 \cdot x^3 + 256 \cdot x^2 + 12 \cdot x + 13$$

where x is the input to your program and z is the output of your program, both x and z are 8-bit positive integers, and all arithmetic is done with 8-bit positive integers. You overheard two of your friends planning to write a program to compute some linear polynomial $z = a_1 \cdot x + a_2$, which they claimed would have the same output as the given cubic polynomial. However, you didn't hear the specific values a_1 and a_2 they discussed.

1. (5 points) Why do your friends think that a linear polynomial can be used in place of the given cubic polynomial? If their program works, what are the smallest positive values possible for a_1 and a_2?

   Answer: Note that $256 = 2^8$ and $2560 = 10 \cdot 2^8$. So, no matter what are x^2 and x^3, they will have no effect on z due to arithmetic modulo 256, i.e. arithmetic with 8-bit integers. The only part that matters is $12x + 13$ which is a linear polynomial. $a_1 = 12$, and $a_2 = 13$.

2. (1 point) Whether or not their program works, do you think this program would run faster using a linear polynomial than using the cubic polynomial? Why?

   Answer: Yes. It avoids computation of $2560 \cdot x^3 + 256 \cdot x^2$ and so performs fewer operations overall. This will make their code faster.

6.2 (14 points) Bob and Alice are lab partners. They are working with the following polynomial (a, b, x are integers):

$$f(x) = ax^6 + (a - b)x^5 + 3^a x^4 + a^2 x^3 + 2ab^2 x^2 + (a + b)x + b^3$$

Bob is performing an experiment in the machine room; his task is to measure parameters a and b, then compute the coefficients of $f(x)$, and send the coefficients to Alice over an unreliable communication channel. Alice is sitting in the computer room; her task is to receive the coefficients that Bob sends, then reconstruct the polynomial $f(x)$. Now suppose the channel can drop at most 4 integers in a message, but does not corrupt any. So, for sending the coefficients Bob and Alice decide to use error correcting codes with polynomials that they learnt in CS 70.

1. (2 points) Since $f(x)$ is a degree-6 polynomial, Bob realizes that he needs to evaluate the polynomial on at least 7 distinct points so that Alice can reconstruct all the coefficients. How many integers should he send to Alice according to the scheme they learnt?

   Answer: $7 + 4 = 11$

2. (2 points) Bob later realizes that all coefficients of $f(x)$ depend only on a and b. He can just send these two integers to Alice. She can compute the coefficients of $f(x)$ herself based on a and b sent by Bob, and this way she can reconstruct $f(x)$ herself. How many integers should Bob send across the channel now?

   Answer: $2 + 4 = 6$

3. (10 points) Suppose Bob has decided to send a and b to Alice across the channel and has told Alice about his decision. Alice now receives the message $(5, -, 11, -, 17, 20)$ from Bob, where the integers in the message are values of a polynomial $ax + b$ at the points 1,2,3,4,5,6, and where '$-$' means that the corresponding integer was dropped

by the channel. Show how she can use Lagrange interpolation to reconstruct the polynomial $f(x)$. Show all your work and the final polynomial $f(x)$.

Answer: Two points are sufficient to reconstruct $ay + b$. Using Lagrange interpolation with points (1, 5) and (3, 11), the polynomial that Bob sent is

$$5 \cdot \frac{y-3}{1-3} + 11 \cdot \frac{y-1}{3-1} = 3y + 2$$

Hence $a = 3, b = 2$. Therefore, Alice will construct the following polynomial

$$\begin{aligned} f(x) &= 3x^6 + (3-2)x^5 + 3^3x^4 + 3^2x^3 + (2 \cdot 3 \cdot 2^2)x^2 + (3+2)x + 2^3 \\ &= 3x^6 + x^5 + 27x^4 + 9x^3 + 24x^2 + 5x + 8 \end{aligned}$$

Question 6 (20 points) Polynomials and Error Correcting Codes.

6.1 (6 points). In a programming assignment, you are asked to write a program that computes

$$z = 256 \cdot y^3 + 2560 \cdot y^2 + 16 \cdot y + 17$$

where y is the input to your program and z is the output of your program, both y and z are 8-bit positive integers, and all arithmetic is done with 8-bit positive integers. You overheard two of your friends planning to write a program to compute some linear polynomial $z = b_1 \cdot y + b_2$, which they claimed would have the same output as the given cubic polynomial. However, you didn't hear the specific values b_1 and b_2 they discussed.

1. (5 points) Why do your friends think that a linear polynomial can be used in place of the given cubic polynomial? If their program works, what are the smallest positive values possible for b_1 and b_2?

   Answer: Note that $256 = 2^8$ and $2560 = 10 \cdot 2^8$. So, no matter what are y^2 and y^3, they will have no effect on z due to arithmetic modulo 256, i.e. arithmetic with 8-bit integers. The only part that matters is $16y + 17$ which is a linear polynomial. $b_1 = 16$, and $b_2 = 17$.

2. (1 point) Whether or not their program works, do you think this program would run faster using a linear polynomial than using the cubic polynomial? Why?

   Answer: Yes. It avoids computation of $256 \cdot y^3 + 2560 \cdot y^2$ and so performs fewer operations overall. This will make their code faster.

6.2 (14 points) Bob and Alice are lab partners. They are working with the following polynomial (c, d, y are integers):

$$g(y) = cy^6 + (c + d)y^5 + 5^c y^4 + d^3 y^3 + 2c^2 y^2 + dy + d^2$$

Bob is performing an experiment in the machine room; his task is to measure parameters c and d, then compute the coefficients of $g(y)$, and send the coefficients to Alice over an unreliable communication channel. Alice is sitting in the computer room; her task is to receive the coefficients that Bob sends, then reconstruct the polynomial $g(y)$. Now suppose the channel can drop at most 4 integers in a message, but does not corrupt any. So, for sending the coefficients Bob and Alice decide to use error correcting codes with polynomials that they learnt in CS 70.

1. (2 points) Since $g(y)$ is a degree-6 polynomial, Bob realizes that he needs to evaluate the polynomial on at least 7 distinct points so that Alice can reconstruct all the coefficients. How many integers should he send to Alice according to the scheme they learnt?

   Answer: 7 + 4 = 11

2. (2 points) Bob later realizes that all coefficients of $g(y)$ depend only on c and d. He can just send these two integers to Alice. She can compute the coefficients of $g(y)$ herself based on c and d sent by Bob, and this way she can reconstruct $g(y)$ herself. How many integers should Bob send across the channel now?

   Answer: 2 + 4 = 6

3. (10 points) Suppose Bob has decided to send c and d to Alice across the channel and has told Alice about his decision. Alice now receives the message $(5, -, -, 11, 13, 15)$ from Bob, where the integers in the message are values of a polynomial $cx+d$ at the points 1,2,3,4,5,6, and where '$-$' means that the corresponding integer was dropped

by the channel. Show how she can use Lagrange interpolation to reconstruct the polynomial $g(y)$. Show all your work and the final polynomial $g(y)$.

Answer: Two points are sufficient to reconstruct $cx + d$. Using Lagrange interpolation with points (1, 5) and (3, 11), the polynomial that Bob sent is

$$5 \cdot \frac{x-4}{1-4} + 11 \cdot \frac{x-1}{4-1} = 2x + 3$$

Hence $c = 2, d = 3$. Therefore, Alice will construct the following polynomial

$$\begin{aligned} g(y) &= 2y^6 + (2+3)y^5 + 5^2y^4 + 3^3y^3 + (2 \cdot 2^2)y^2 + 3y + 3^2 \\ &= 2y^6 + 5y^5 + 25y^4 + 27y^3 + 8y^2 + 3y + 9 \end{aligned}$$