Midterm 1

7:00-9:00pm, 8 October

Notes: There are **five** *questions on this midterm. Answer each question part in the space below it, using the back of the sheet to continue your answer if necessary. If you need more space, use the blank sheet at the end. In both cases, be sure to clearly label your answers!* **None of the questions requires a very long answer, so avoid writing too much! Unclear or long-winded solutions may be penalized.** *The approximate credit for each question part is shown in the margin (total 100 points). Points are not necessarily an indication of difficulty!*

Your Name: **Your Section:**

Person on left: **Person on right:**

For official use; please do not write below this line! For official use; please do not write below this line!

Q1	16
Q2	20
Q3	20
Q4	14
Q5	15 + 15
Total	100

[exam starts on next page]

1. [Propositional Logic] [16 pts]

A. (8 pts - 2 pts each) State whether the following equivalences are valid or invalid. There is no need to justify your answers. Guess at your own risk - wrong answers will be awarded negative credit.

I. $\neg\forall n\,[(P(n) \wedge Q(n)) \Rightarrow \neg R(n)] \equiv \exists n\,[P(n) \wedge Q(n) \wedge R(n)]$

Solution: This equivalence is valid. We can show this by applying DeMorgan's law and using the fact that $P \Rightarrow Q \equiv \neg P \vee Q$.

$$\begin{aligned}
\neg\forall n\,[(P(n) \wedge Q(n)) \Rightarrow \neg R(n)] &\equiv \neg\forall n\,[\neg(P(n) \wedge Q(n)) \vee \neg R(n)] \\
&\equiv \exists n \neg\,[\neg(P(n) \wedge Q(n)) \vee \neg R(n)] \\
&\equiv \exists n\,[(P(n) \wedge Q(n)) \wedge R(n)] \\
&\equiv \exists n\,[P(n) \wedge Q(n) \wedge R(n)]
\end{aligned}$$

II. $\forall m\,\exists n\,[\forall l(A(m,l) \wedge B(n,l)) \Rightarrow C(m,n)] \equiv \forall m\,\exists n\,[\neg C(m,n) \Rightarrow \exists l(\neg A(m,l) \vee \neg B(n,l))]$

Solution: This equivalence is valid. We can show this by using the fact that an implication and its contrapositive are equivalent, that is $P \Rightarrow Q \equiv \neg Q \Rightarrow \neg P$, and by using DeMorgan's law.

$$\begin{aligned}
\forall m\,\exists n\,[\forall l(A(m,l) \wedge B(n,l)) \Rightarrow C(m,n)] &\equiv \forall m\,\exists n\,[\neg C(m,n) \Rightarrow \neg(\forall l(A(m,l) \wedge B(n,l)))] \\
&\equiv \forall m\,\exists n\,[\neg C(m,n) \Rightarrow \exists l(\neg A(m,l) \vee \neg B(n,l))]
\end{aligned}$$

III. $\forall m\,\forall n\,[P(m) \Rightarrow Q(n)] \equiv \forall n\,\forall m\,[Q(n) \Rightarrow P(m)]$

Solution: This equivalence is invalid. That is because an implication and its converse are not necessarily equivalent, that is $P \Rightarrow Q \not\equiv Q \Rightarrow P$.

IV. $\neg\forall l\,\exists m\,\forall n\,[(P(m) \wedge Q(l)) \vee R(m,n,l)] \equiv \exists l\,\forall m\,\exists n\,[(\neg P(m) \wedge \neg Q(l)) \vee \neg R(m,n,l)]$

Solution: This equivalence is invalid. It involves an incorrect application of DeMorgan's law (it does not flip the or into an and).

$$\begin{aligned}
\neg\forall l\,\exists m\,\forall n\,[(P(m) \wedge Q(l)) \vee R(m,n,l)] &\equiv \exists l\,\forall m\,\exists n \neg\,[(P(m) \wedge Q(l)) \vee R(m,n,l)] \\
&\equiv \exists l\,\forall m\,\exists n\,[\neg(P(m) \wedge Q(l)) \wedge \neg R(m,n,l)] \\
&\equiv \exists l\,\forall m\,\exists n\,[(\neg P(m) \vee \neg Q(l)) \wedge \neg R(m,n,l)] \\
&\not\equiv \exists l\,\forall m\,\exists n\,[(\neg P(m) \wedge \neg Q(l)) \vee \neg R(m,n,l)]
\end{aligned}$$

B. (8 pts - 2 pts each) For nonnegative integers x and y, let $P(x,y)$ be the proposition that "$x + y > xy$" . Which of the following statements are true? Give a one line proof or a counterexample.

I. $\forall x\,\exists y P(x,y)$

Solution: This statement is true. A simple way to show this is to say that for every value of x, we pick $y = 1$. Then, $P(x,y)$ is always true since $x + 1 > x$ for all x.

II. $\exists x \, \exists y P(x, y)$

Solution: This statement is true. To show this we just need to find x and y that satisfy the property $P(x, y)$. We can just pick $x = y = 1$; then we can see that $1 + 1 = 2 > 1 = 1 \cdot 1$.

III. $\exists x \, \forall y P(x, y)$

Solution: This statement is true. A simple way to show this is to say that we pick $x = 1$. Then, for every value of y, $P(x, y)$ is true since $y + 1 > y$ for all y.

IV. $\forall x \, \forall y P(x, y)$

Solution: This statement is false. A simple way to show this is to pick a counterexample. We pick $x = y = 3$. Then we have $6 = 3 + 3 \not> 9 = 3 \cdot 3$.

2. [Proofs.] [20 pts]

A. (10 pts) Let D_n be the number of ways to tile a $2 \times n$ checkerboard with dominos, where a domino is a 1×2 piece. Prove that $D_n \leq 2^n$ for all positive integers n. (Find a recurrence relation for D_n. No need to give a proof. Then inductively prove the upper bound on D_n.)

Note that dominos can only be placed exactly aligned with checkerboard squares, and cannot be placed diagonally.

Solution: First we need to come up with a recurrence relation for D_n. Consider the case when $n \geq 3$; we want to break down the case when we have a $2 \times n$ size checkerboard to smaller cases. If we start tiling from the end of the board, we see that there are two possibilities - either we put a domino on horizontally, in which case we are left with a board of size $2 \times n - 1$, or we can put on two dominos vertically, in which case we are left with a board of size $2 \times n - 2$. So, our relation is $D_n = D_{n-1} + D_{n-2}$. Now we prove that $D_n \leq 2^n$.
Base Case: In this situation it is easier if we use 2 base cases. First, consider the case when $n = 1$. There is exactly one way to tile such a checkerboard, so $D_1 = 1 \leq 2$. Next, consider the case when $n = 2$. We can either tile this checkerboard with two horizontal dominos or two vertical dominos. So $D_2 = 2 \leq 4$.
Induction Hypothesis: Assume that $D_n \leq 2^n$, for all $n \leq k$. We want to show that it is true for $n = k + 1$.
Induction Step: We combine our recurrence relation and the induction hypothesis to get:

$$\begin{aligned} D_{k+1} &= D_k + D_{k-1} \\ &\leq 2^k + 2^{k-1} \\ &\leq 2^k + 2^k \\ &= 2^{k+1} \end{aligned}$$

So we have shown that $D_{k+1} \leq 2^{k+1}$ and thus we know that $D_n \leq 2^n$ for all positive integers n, and so we are done.

B. (10 pts) Show that $\forall$ odd $a \in N, a^2 = 1 \mod 8$.

Solution: An easy way to prove this is just to show that this is true for $a = 1, 3, 5, 7$. Because of the properties of arithmetic modulo 8, all odd numbers modulo 8 are equivalent to either $1, 3, 5$, or 7. Because of this fact, if we show it is true for these four numbers, then we have shown it to be true for all odd $a \in N$. So we get

$$\begin{aligned} 1^2 &= 1 \mod 8 \\ 3^2 &= 9 \mod 8 \\ &= 1 \mod 8 \\ 5^2 &= 25 \mod 8 \\ &= 1 \mod 8 \\ 7^2 &= 49 \mod 8 \\ &= 1 \mod 8 \end{aligned}$$

Alternate Solution: Since an odd natural number is defined as $2k + 1$ for some $k \in N$, we need to prove that $\forall k \in N, (2k + 1)^2 = 1 \mod 8$.

Base Case: $k = 0$. Then $(2k+1)^2 = 1 = 1 \mod 8$.
Induction Hypothesis: Assume that $(2k+1)^2 = 1 \mod 8$. We want to show that $(2(k+1)+1)^2 = 1 \mod 8$.
Induction Step: We have

$$\begin{aligned}
(2(k+1)+1)^2 &= (2k+3)^2 \\
&= 4k^2 + 12k + 9 \\
&= (4k^2 + 4k + 1) + 8k + 8 \\
&= (2k+1)^2 + 8(k+1) \\
&= 1 + 0 \mod 8 \\
&= 1 \mod 8
\end{aligned}$$

Thus, $\forall k \in N, (2k+1)^2 = 1 \mod 8$.

3. [RSA] [20 pts]

A. (10 pts) $e = 7, p = 7, q = 11$ Find d.

Solution: Remember that from the way RSA is setup that $d = e^{-1} \mod (p-1)(q-1)$. So we are looking for $d = 7^{-1} \mod 60$. In order to find this, we use the extended GCD algorithm with inputs 60 and 7.

```
egcd(60, 7)
  egcd(7, 4)
    egcd(4, 3)
      egcd(3, 1)
        egcd(1, 0)
        return (1, 1, 0)
      return (1, 0, 1)
    return (1, 1, 0 - (4 div 3) x 1) = (1, 1, -1)
  return (1, -1, 1 - (7 div 4) x (-1)) = (1, -1, 2)
return (1, 2, -1 - (60 div 7) x 2) = (1, 2, -17)
```

We can read off from here that $d = -17 = 43 \mod 60$.

B. (5 pts) With RSA Amazon can *sign* a message as follows; For a system with public key (N, e) and secret key d, Amazon sends the message $(x, x^d \mod N)$. If Bob gets (x, y), how can he verify that $y = x^d \mod N$? (Bob does not know d and the answer is very brief.)

The answer that we were looking for is very simple. If Bob receives (x, y) and knows (N, e), one way that he could verify that $y = x^d$ is simply to encrypt the message y. If $y = x^d$, we get:

$$\begin{aligned} E(x^d) &= (x^d)^e \mod N \\ &= x^{de} \mod N \\ &= x^{1+k(p-1)(q-1)} \mod N \\ &= x \mod N \end{aligned}$$

This was shown all with properties that we learned from RSA. So, if $E(y) = x$, then we know that the message (x, y) was sent by Amazon.

C. (5 pts) Use the fact that $a^{p-1} = 1 \mod p$ for prime p and a relatively prime to p to prove that $a^{(p-1)(q-1)} = 1 \mod pq$ for primes p and q and a relatively prime to p and q.

From the fact that $a^{p-1} = 1 \mod p$, we can see that:

$$\begin{aligned} a^{(p-1)(q-1)} &= (a^{p-1})^{q-1} \mod p \\ &= 1^{q-1} \mod p \\ &= 1 \mod p \end{aligned}$$

Similarly, we see that $a^{(p-1)(q-1)} = 1 \mod p$. So, from this we can see that:

$$\begin{aligned} a^{(p-1)(q-1)} - 1 &= jp \\ a^{(p-1)(q-1)} - 1 &= kq \end{aligned}$$

So, $jp = kq$. From this we can see that p divides kq. However, since p and q are distinct, they are relatively prime to each other. Therefore, k must be a multiple of p - let's call it mp. So we get

$$\begin{aligned} a^{(p-1)(q-1)} - 1 &= mpq \\ a^{(p-1)(q-1)} &= 1 + mpq \\ a^{(p-1)(q-1)} &= 1 \mod pq \end{aligned}$$

We noticed a lot of people tried to use the Chinese remainder theorem to solve this problem. Since the Chinese Remainder Theorem was not covered in lecture or the homework, and was only mentioned once in the section notes, we only accepted answers that were very complete when they used the Chinese Remainder Theorem. Here is what we were looking for.

The Chinese remainder theorem states that if a number modulo pq is uniquely determined by its value modulo p and q. That is, given a and b, that there is a unique number x modulo pq such that $x = a \mod p$ and $x = b \mod q$. So, in this problem, we first expected you to show that $a^{(p-1)(q-1)} = 1 \mod p$ and $a^{(p-1)(q-1)} = 1 \mod q$. Also, you would need to state that $1 = 1 \mod p$ and $1 = 1 \mod q$. Then, by the Chinese remainder theorem, since there is a unique number modulo pq that is equivalent to 1 modulo p and 1 modulo q, we must have that $a^{(p-1)(q-1)} = 1 \mod pq$.

4. [Stable Marriage] [14 pts]

A. (8 pts) 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 are

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

Use the traditional marriage algorithm to find the male-optimal pairing.

Day	1	2	3
A:	**1**	**1**	**1**
B:			**2**
C:	**2**	2, **4**	**4**
D:	**3**, 4	**3**	**3**

So, the male-optimal pairing is $(A, 1), (B, 2), (C, 4), (D, 3)$.

B. (3 pts) Given n men and n women, what is the minimum number of stable pairings that must exist for any set of preferences? Justify your answer by describing an instance.

The minimal number of stable pairings is 1. This happens when the male-optimal and female-optimal pairings are the same. An example of this is when man 1 and woman A have each other on the top of their list, man 2 and woman B have each other on the top of their list, and so on. The only stable pairing in this instance is $(1, A), (2, B), \ldots$.

It was necessary to describe an instance that works for arbitrary n to receive full credit.

C. (3 pts) We saw in the homework that it was possible for a pairing to be stable even if there was a pair (M, W) such that M was W's least favorite man and W was M's least favorite woman. What is the maximum number of couples with this property (each member is paired with their least favored partner) can there be in any stable pairing? Justify your answer.

The maximum number is 1; suppose that this is not true - that there is a situation where we have a stable paring that has at least two such couples - call them $(1, A)$ and $(2, B)$. In this situation we know that 1 and A have each other on the bottom on their preference lists, and 2 and B have each other on the bottom of their preference lists. So, from this we know that 1 must prefer B over A, and 2 must prefer 1 over 2. Therefore, $(1, B)$ is a rogue couple, which contradicts the fact that the pairing was stable. Thus, we have a contradiction, and there can be at most one such couple with this property in any stable pairing.

5. [Codes] [30 pts]

A. (15 pts) Your friend sends you a message in the alphabet R = 0, F = 1, A = 2, U = 3, and N = 4 using the polynomial scheme discussed in class. Assume that a polynomial $P(\cdot)$ over $GF(q)$ is used, for the smallest value of q that will accommodate the given alphabet. The message size is 3. Four packets are sent where packet i (starting from 0) corresponded to $P(i)$. You receive the following packets.

- F
- U
- clearly corrupted
- N

Assuming the three decipherable packets arrive uncorrupted, what is the value in the corrupted packet? Justify your answer.

The smallest q that will accommodate our size 5 alphabet is $q = 5$. So we will do everything modulo 5. From the information given, we know that three of the points of $P(\cdot)$ are $(0, 1)$, $(1, 3)$, and $(3, 4)$. We know that $P(\cdot)$ is a degree 2 polynomial, since the message was of size 3. And since we have 3 points of $P(\cdot)$, we can recover $P(\cdot)$ exactly using polynomial interpolation. Remember that we do everything modulo 5 and that instead of dividing we multiply by the inverses modulo 5. We get:

$$\begin{aligned}
\Delta_0(x) &= \frac{(x-1)(x-3)}{(0-1)(0-3)} \\
&= \frac{x^2-4x+3}{3} \\
&= 2(x^2-4x+3) \\
&= 2x^2-8x+6 \\
&= 2x^2+2x+1 \\
\Delta_1(x) &= \frac{(x-0)(x-3)}{(1-0)(1-3)} \\
&= \frac{x^2-3x}{-2} \\
&= 2(x^2-3x) \\
&= 2x^2-6x \\
&= 2x^2+4x \\
\Delta_3(x) &= \frac{(x-0)(x-1)}{(3-0)(3-1)} \\
&= \frac{x^2-x}{6} \\
&= 1(x^2-x) \\
&= x^2+4x \\
P(x) &= 1\Delta_0(x)) + 3\Delta_1(x) + 4\Delta_3(x) \\
&= 2x^2+2x+1+6x^2+12x+4x^2+16x \\
&= 2x^2+1
\end{aligned}$$

Now we can use $P(x)$ to recover the corrupted packet: it is $P(2) = 9 = 4 =$ N. So the original message was FUN.

B. Say another message is sent using five packets and you receive packets F, U, N, U, and R, one of which is wrong.

I. (7 pts) The original message is either "FUN" or "RUN". Which is it? Why? (Hint: try one.)

Since we already know what the encoding polynomial looks like if the original message was FUN, let's start by assuming that the original message was FUN. This means that $P(x) = 2x^2 + 1$, and we know that there is only one corrupted packet. Since the original message was FUN, this means that the first three packets were sent through uncorrupted. The fourth packet is corrupted - it should have been $P(3) = 4 =$ N, but we received a U instead. However, the fifth packet is also corrupted - it should have been $P(4) = 3 =$ U, but we received an R instead. Therefore, the original message could not have been FUN, and thus the original message must have been RUN.

II. (4 pts) Recall that in the Berlekamp-Welch algorithm, one can set up a set of linear equations and use the solution to reconstruct the original polynomial. How many unknowns and equations do you have in the Berlekamp-Welch system for this situation?

Recall that in Berlekamp-Welch we are trying to solve for the coefficients of $Q(x)$ and $E(x)$. $Q(x)$ is an $n - 1 + k$ degree polynomial - in this case it would be a $3 - 1 + 1 = 3$ degree polynomial, and thus it has 4 unknown coefficients. $E(x)$ is a degree k polynomial, but we already know that its highest order coefficient is 1. In this case it is a degree 1 polynomial, and thus it has 1 unknown coefficient. Thus there are 5 unknowns and equations total.

III. (4 pts) Write out the equations that correspond to the first two received characters: i.e., $R(0)$ and $R(1)$. Denote the coefficients of $Q(x)$ using a_i and the coefficients of $E(x)$ by b_i.

From above, we know that the form of $Q(x)$ and $E(x)$ are:

$$\begin{aligned} Q(x) &= a_3x^3 + a_2x^2 + a_1x^2 + a_0 \\ E(x) &= x + b_0 \end{aligned}$$

We also know that $Q(i) = R(i)E(i)$; so for $i = 0, 1$ we get:

$$\begin{aligned} 0a_3 + 0a_2 + 0a_1 + a_0 &= 1(0 + b_0) \\ a_0 - b_0 &= 0 \end{aligned}$$

And:

$$\begin{aligned} a_3 + a_2 + a_1 + a_0 &= 3(1 + b_0) \\ a_3 + a_2 + a_1 + a_0 - 3b_0 &= 3 \end{aligned}$$