Midterm 1

Name:

TA:

Answer all questions. Read them carefully first. Be precise and concise. The number of points indicate the amount of time (in minutes) each problem is worth spending. Write in the space provided, and use the back of the page for scratch. *Good luck!*

Problem 1

(Short questions *and answers*, 50 points total)

1. (3 points) You are proving by contrapositive (*not* by contradiction) the statement "If x is prime, then $x+7$ is not a prime." You start your proof as follows (circle one option from each set):

   "Suppose that { x / $x+7$ } { is / is not } a prime."

   Solution: The contrapositive of $A \Rightarrow B$ is $\neg B \Rightarrow \neg A$, so in this case that is "Suppose that $x+7$ is prime..."

2. (3 points) Now suppose that, instead, you want to prove this statement by cases. Which two cases would you consider?

   Solution: With a proof by cases we are assuming the hypothesis "x is prime" and trying to prove the consequence "$x+7$ is not prime". The cases that are most conducive to a proof are: Case 1) x is an even prime and Case 2) x is an odd prime. [The proof then proceeds: if x even prime, then $x=2$ so $x+7=9$ is not prime. If x an odd prime, the $x+7$ is the sum of two odd numbers, so it is even and therefore divisible by 2. It is bigger than 2, so it cannot be prime.

3. (8 points) Suppose that $P(x,y)$ is the following property of integers x and y: "$x = y+y$ or $x = y+y+1$." For each of these statements state if it is true or false. Give a very brief explanation in each case.

   - $\exists x \exists y P(x,y)$

     Solution: True. $x=2$ and $y=1$ satisfy $P(2,1)$ since $2 = 1+1$ so these x and y witness the existential quantifiers.

   - $\exists x \forall y P(x,y)$

     Solution: False. For any x, we have $\neg P(x, x+10)$ since no integer x satisfies $x = x+10+x+10$ or $x = x+10+x+10+1$. Thus, no x can exist to make $P(x,y)$ true for all y since we have provided a counterexample for each possible x.

   - $\forall x \exists y P(x,y)$

     Solution: True. Given x, if x is even, choose $y = x/2$. Then $x = y+y$. If x is odd, choose $y = (x-1)/2$. Then $x = y+y+1$. In both cases y is an integer and $P(x,y)$ holds, so we have shown that for every x there is a y to make $P(x,y)$ true.

   - $\forall x \forall y P(x,y)$

     Solution: False. Again, for any x we have $\neg P(x, x+10)$, so $P(x,y)$ is not true for all x and all y. This can also be seen from the falsehood of the second statement: if the current statement were true, then in particular for $x=1$ we would have $\forall y P(1,y)$ and so $x=1$ would make the second statement true, a contradiction.

   - $\forall y \exists x P(x,y)$

     Solution: True. Given y, set $x = y+y$. Then $P(y+y, y)$ is true by definition. So for every y we are able to find a corresponding x to make $P(x,y)$ true.

4. (4 points) Write the negation of the following statement,
$\forall y \exists x$ $[x = y + y$ or $x = y + y + 1]$
so that there are no negation signs (so use $\neq$ as appropriate).

Solution:

$$\neg\forall y\exists x[x = y + y \vee x = y + y + 1]$$
$$\exists y\forall x\neg[x = y + y \vee x = y + y + 1]$$
$$\exists y\forall x[x \neq y + y \wedge x \neq y + y + 1]$$

5. (6 points) For each of the following integers find its inverse modulo 35, or state that it does not exist (explain briefly why it doesn't exist).

   - 4
     Solution: $4 * 9 = 36 \equiv 1 \mod 35$ so 9 is the inverse of 4 modulo 35.
   - 14
     Solution: $\gcd(14, 35) = 7 \neq 1$ so therefore 14 does not have an inverse modulo 35.
   - 34
     Solution: $34 \equiv -1 \mod 35$ so since $(-1)^2 = 1$ we know that $-1 = 34$ is the inverse of 34 modulo 35. In other words, 34 is its own inverse.

6. (3 points) What is the gcd of the integers 28 and 5? Find integers (possibly negative) x and y such that $28x + 5y = 2$, or state that no such integers exist. Explain briefly.

   Solution: Run the extended gcd algorithm to find $d = \gcd(28, 5)$ and also x', y' such that $28x' + 5y' = d$.

   $(d, x', y') = egcd(28, 5)$
   $(d_1, x_1, y_1) = egcd(5, 3)$
   $(d_2, x_2, y_2) = egcd(3, 2)$
   $(d_3, x_3, y_3) = egcd(2, 1)$
   $(d_4, x_4, y_4) = egcd(1, 0)$
   $(d_4, x_4, y_4) = (1, 1, 0)$
   $(d_3, x_3, y_3) = (d_4, y_4, x_4 - y_4\lfloor\frac{2}{1}\rfloor) = (1, 0, 1)$
   $(d_2, x_2, y_2) = (d_3, y_3, x_3 - y_3\lfloor\frac{3}{2}\rfloor) = (1, 1, -1)$
   $(d_1, x_1, y_1) = (d_2, y_2, x_2 - y_2\lfloor\frac{5}{3}\rfloor) = (1, -1, 2)$
   $(d, x', y') = (d_1, y_1, x_1 - y_1\lfloor\frac{28}{5}\rfloor) = (1, 2, -11)$

   So $28 \cdot 2 + 5 \cdot (-11) = 1$. Multiply through by 2 to get $28 \cdot 4 + 5 \cdot (-22) = 2$, which means $x = 4$ and $y = -22$ work.

7. (3 points) How many polynomials $p(x)$ of degree 4 modulo 7 are there such that $p(1) = p(2) = p(3) = 0 \mod 7$?

   Solution: A polynomial of degree 4 is determined uniquely by 5 values. Since $p(1), p(2)$, and $p(3)$ are already set to 0, we have freedom in determining $p(4)$ and $p(5)$. For each pair of values x and y we assign to $p(4)$ and $p(5)$ we get a unique polynomial of degree 4, so the number of polynomials equals the number of pairs (x, y) we can find modulo 7. We can choose x and y independently and they come from the seven numbers $\{0, 1, 2, 3, 4, 5, 6\}$ which are the unique classes modulo 7. So there are $7 \times 7 = 49$ polynomials of degree 4 that meet our specified conditions.

8. (4 points) My packets are integers between 1 and 1,000,000, and they are labeled so I know which were dropped. If I want to encode 10 packets by polynomials and I know that only 3 will be dropped, what degree polynomial should I use? And modulo what kind of number?

   Solution: We want to send $n = 10$ packets, but since $k = 3$ packets will be dropped with every transmission, we have to send $n + k = 13$ packets to assure the information will get through. The recipient will get 10 of the 13 packets we sent, and he/she has to use this to recover the remaining 3 packets. He/she can do this because 10 points determine a unique polynomial of degree 9. So we want to use a polynomial of degree 9 to encode our packets. Furthermore, we always work modulo a *prime number* that is sufficiently big. How big? It has to be bigger than the number of packets we want to send (13), as well as bigger than the largest possible value a packet can have (1,000,000). So we need to work modulo a prime number greater than 1 million.

9. (4 points) Is 0011 a de Bruijn sequence of order 2? How about 0101? Explain briefly.

   Solution: 0011 is a de Bruijn sequence, and 0101 is not. Since if we wrap 0011 around, we can find all possible two bit strings $00, 01, 10, 11$ exactly once in it.

10. (6 points) A graph has 6 nodes, 9 edges, and no triangles. Can it be planar? Explain briefly.

    Solution: Remember that planar graph must satisfies Euler's formula $v + f = e + 2$. Suppose this graph is a planar, since there is no triangles, every face consists of four or more edges. And since every edge is shared by two faces we can get that $f \leq \frac{2e}{4}$. Substituting this back to Euler's formula, we can get $2v + e \geq 2e + 4$ which is $2v \geq e + 4$. Now we have 6 nodes and 9 edges, $2 \times 6 \not\geq 9 + 4$, a contradiction!

11. (3 points) How many different ways are there to seat a class of 140 into a lecture room with 160 seats? (Two seatings are considered different if there is a student who sits in a different chair in the two.) Factorials are OK.

    Solution: We can first choose 140 seats out of the 160 seats without ordering and then seat 140 students with ordering. Therefore, there are

    $$\binom{160}{140} \times 140! = \frac{160!}{20!}$$

    ways.

12. (3 points) How many bitstrings of length 160 are there that have 140 ones?

    Solution: 140 of the 160 bits are one, and 20 of the 160 are zero. So we can choose 140 bits out of the 160 bits and set them to 1. Or equivelently choose 20 bits out of the 160 bits and set them to 0. Therefore, there are

    $$\binom{160}{140} = \binom{160}{20}$$

    different bitstrings.

13. ($\frac{1}{2}$ points extra credit) What is $(x - a) \cdot (x - b) \cdot (x - c) \cdots (x - z)$? (Be very brief.)

    Solution: 0 because $(x - x)$ is one of these terms.

Problem 2

(*10 points)* Prove by induction that, for any integer $n \geq 1$, $\sum_{k=1}^{n} k \cdot k! = (n+1)! - 1$.

Basis:
Solution: For $n = 1$,

$$\begin{aligned} \sum_{k=1}^{1} k \cdot k! &= 1 \times 1! \\ &= 1 \\ &= (1+1)! - 1. \end{aligned}$$

Induction hypothesis:
Solution: Assume that for some $n = l \geq 1$, $\sum_{k=1}^{l} k \cdot k! = (l+1)! - 1$.

Induction step:
Solution: For $n = l + 1$,

$$\begin{aligned} \sum_{k=1}^{l+1} k \cdot k! &= (l+1) \times (l+1)! + \sum_{k=1}^{l} k \cdot k! \text{ by spliting the sum} \\ &= (l+1) \times (l+1)! + [(l+1)! - 1] \text{ by induction hypothesis} \\ &= (l+1+1) \times (l+1)! - 1 \text{ by collecting the first two terms} \\ &= (l+2) \times (l+1)! - 1 \\ &= (l+2)! - 1. \end{aligned}$$

Therefore, by induction, $\forall n \geq 1$, $\sum_{k=1}^{n} k \cdot k! = (n+1)! - 1$.

Problem 3

(*10 points)*
A: abc
B: abc
C: acb

a: ABC
b: BCA
c: CBA

Consider the preferences by the three boys (small letters) and girls (caps) above. Which of the following matchings are stable and which are unstable? If unstable, give a rogue pair. If stable, state whether the matching is man-optimal and/or woman-optimal.

1. a-A, b-B, c-C

   Solution: This pairing is stable. This is because there is no pair who mutually prefers each other over their assigned partners. Also, this pairing happens to be both man-optimal and woman-optimal. To see this, we first remember that running the TMA always gives us a stable pairing which is man-optimal. This algorithm finishes with one iteration, as shown below:

	1
a	A
b	B
c	C

   Next, we remember that if we run the reverse-TMA algorithm (when the women propose to the men), we always get a stable pairing which is woman-optimal. The algorithm finishes in two iterations, as shown below:

	1	2
A	**a**	a
B	a	b
C	a	c

   In both cases we end up with the matching in question, so it is stable, man-optimal, and woman-optimal.

2. a-B, b-A, c-C

   Solution: This pairing is unstable. This is because there is a rogue pair: (a, A). They are a rogue pair because a prefers A more than his partner B and A also prefers a more than her partner b.

3. a-A, b-C, c-B

   Solution: This pairing is unstable. This is because there is a rogue pair: (b, B). They are a rogue pair because b prefers B more than his partner C and B also prefers b more than her partner c. The same argument can be used to show that (c, C) is also a rogue pair.

Problem 4

(*10 points)* Three families with three people in each, call them $\{A, B, C\}, \{D, E, F\}, \{G, H, J\}$, share an electronic safe deposit box. They want the box to open only if at least two members from each of at least two families are present. For example, if A, B, D, E are present then the box should open, but not if A, B, C, E, G are present. Explain how this can be done. How many polynomials and of which degree would you use? (Hint: look for a "hierarchical" version of secret sharing.)

The idea here is that we want to make some kind of hierarchical scheme - we want two families to be able to unlock the secret of the safe, and we want two family members in each family to be to unlock the secret of it's family (which is then used to unlock the safe). To accomplish this, we are going to use polynomials in some kind of hierarchical sense.

To begin, suppose that the secret to opening the safe is to know some secret code s. Since we want any two of the three families to be able to recover it, let's encode this into some one dimensional polynomial such that $p(x)$ such that $p(0) = s$. We then assign the value $p(1)$ to family 1, $p(2)$ to family 2 and $p(3)$ to family 3.

But wait! We do not want to just give the secret family values to all the members of a particular family - then any two people would be able to open the safe, as long as they are from different families. Instead, for each family i, we encode it's secret value $p(i)$ in another one dimensional polynomial $q_i(x)$ such that $q_i(0) = p(i)$. We then give $q_i(1)$, $q_i(2)$, and $q_i(3)$ the first, second, and third member of that family respectively.

So now we see that we have a scheme where we need at least two members from each of at least two families are present. We need two families present in order to recover the secret code of the safe from their secret family keys, and we need two people from each family in order to recover their secret family keys.

An important thing to note is that when finding polynomials to fit this scheme, it is important to start by first finding $p(x)$, instead of first finding $q_1(x)$, $q_2(x)$, and $q_3(x)$. The reason is that if we do it the other way, there is no guarantee that $q_1(0)$, $q_2(0)$, and $q_3(0)$ can all be points on a linear function (for instance, if it were $(1, 0, 1)$).

Problem 5

(*15 points)* In RSA, $p = 5, q = 7$.

1. How many legitimate choices for e are there?

Solution: In RSA, the private exponent e must be coprime with $(p-1)(q-1)$. Here, $(p-1)(q-1) = 4 \cdot 6 = 24 = 2^3 \cdot 3$. So the gcd of e and $(p-1)(q-1)$ is 1 is and only if e is not divisible by either 2 or 3. The admissible values for e are $1, 5, 7, 11, 13, 17, 19$, and 23, from which we exclude 1 (if $e = 1$ then the message is not hidden at all!), so there are 7 possibilities for e.

2. Choose $e = 17$, and give the corresponding d.

Solution: d is the inverse of e modulo $(p-1)(q-1) = 24$. Running the extended-gcd algorithm on $x = 24$ and $y = 17$ gives the following

x	y	a	b
24	17	5	-7
17	7	-2	5
7	3	1	-2
3	1	0	1
1	0	1	0

From this computation we get the relation $5 \cdot 24 - 7 \cdot 17 = 1$, or equivalently $17 \cdot (-7) = 1 + (-5) \cdot 24$ which implies that $17 \cdot (-7) \equiv 1 \mod 24$: the inverse of 17 mod 24 is -7, which is also $-7 + 24 \equiv 17 \mod 24$. The decoding key is therefore $d = 17$.

3. What is the encoding of the message $x = 2$?

Solution: By definition, the encoding of $x = 2$ is

$$\begin{aligned} c &= x^e \mod pq \\ &= 2^{17} \mod 35 \\ &= (2^8 \mod 35)^2 \cdot 2 \mod 35 \\ &= (256 \mod 35)^2 \cdot 2 \mod 35 \\ &= 11^2 \cdot 2 \mod 35 \\ &= 242 \mod 35 \\ &= 32 \end{aligned}$$

4. What is $100^{100} \bmod 35$?

Solution: The extension of Fermat's little theorem says that if p and q are two distinct primes both bigger than 2, then for any a we have that $a^{(p-1)(q-1)} \equiv 1 \mod pq$. In our case $p = 5$ and $q = 7$, so we have that

$a^{24} \equiv 1 \mod 35$ for any a. Take $a = 100$, then $100^{24} \equiv 1 \mod 35$, and elevating to the power 4 we get that $(100^{24})^4 \equiv 1^4 \equiv 1 \mod 35$, or equivalently $100^{96} \equiv 1 \mod 35$. Therefore

$$\begin{aligned}
100^{100} \mod 35 &= 100^{96} \cdot 100^4 \mod 35 \\
&= 1 \cdot (100 \mod 35)^4 \mod 35 \\
&= 30^4 \mod 35 \\
&= (30^2 \mod 35)^2 \mod 35 \\
&= (900 \mod 35)^2 \mod 35 \\
&= 30^2 \mod 35 \\
&= 30
\end{aligned}$$