# CS 70 Discrete Mathematics and Probability Theory
# Summer 2015 Chung-Wei Lin Midterm 1

PRINT Your Name: _____, _____
(last) (first)

SIGN Your Name: _____

PRINT Your Student ID: _____

CIRCLE your exam room: 2050 VLSB 10 EVANS OTHER

Name of the person sitting to your left: _____

Name of the person sitting to your right: _____

- After the exam starts, please write your student ID (or name) on every odd page (we will remove the staple when scanning your exam).
- We will not grade anything on the extra pages (Pages 14–16) or outside of the space provided for a problem unless we are clearly told in the space provided for the question to look there.
- Except special notices, you must show your work to get credits.
- You may consult one single-sided sheet of notes. Apart from that, you may not look at books, notes, etc. Calculators, phones, and computers are not permitted.
- You have 110 minutes. There are 9 questions for a total of 100 points plus 15 bonus points. Use the number of points as a rough guide for the amount of time to allocate to that question. Note that the last two questions (8 and 9) are harder than the rest, so you should attempt it only after you take a good shot at the rest (and don't feel bad if you cannot get them).
- There are 16 pages (sides) on the exam. Notify a proctor immediately if a page is missing.

Do not turn this page until your instructor tells you to do so.

SID:

**1. TRUE or FALSE — First Round (8 points, 1 point for each part)**

For any proposition $P, Q, R$ and $x, y \in \mathbb{R}$, determine whether the following statements are true or false. Just circle the correct choice. No explanation is required. No partial credit will be given.

$T$ $F$ $(P \Longrightarrow Q) \Longrightarrow (Q \Longrightarrow P)$.

$T$ $F$ $(P \vee \neg P)$.

$T$ $F$ $\neg(P \wedge Q) \Longleftrightarrow (\neg P \vee \neg Q)$.

$T$ $F$ $((P \Longrightarrow Q) \wedge (Q \Longrightarrow R)) \Longrightarrow (P \Longrightarrow R)$.

$T$ $F$ $\neg(\forall x\, P) \Longleftrightarrow \exists x\, (\neg P)$.

$T$ $F$ $\forall y \exists x\, P \Longrightarrow \exists x \forall y\, P$.

$T$ $F$ "$(x = 0 \vee y = 0)$ is true" means there exists exactly one of $x$ and $y$ being 0.

$T$ $F$ In $\mathbb{R}$, 2015 points can determine a unique polynomial of degree 2014.

**2. Counting Minions and Bananas (6 points, 3 points for each part)**

For the following two parts, just write down your answers. You do not need to calculate the exact value of $\binom{a}{b}$ or $a!$. No explanation is required. No partial credit will be given.

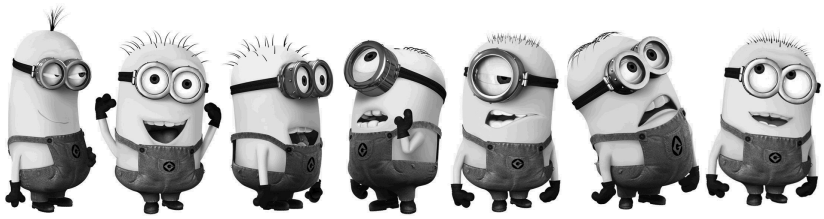

Figure 1: They are Kevin, Bob, Stuart, ... [http://scifi.stackexchange.com/].

(a) There are 7 different minions in the figure. Three of them are going to form a team and find their new master. How many different ways to form the team, where one member has exactly one eye and the other two members have two eyes?

(b) How many different anagrams of BANANA are there?

**3. Conceptual Questions (10 points, 1/1/2/3/3 points for each part)**

(a) Kevin and Bob decide to apply the RSA cryptography so that Kevin can send a secret message to Bob. There are several important variables, $p, q, N, e, d$, defined in the RSA cryptography. Which of them are public? (No explanation is required. No partial credit will be given.)

(b) Following Part (a), let's switch to private variables. Are those private variables kept by Kevin only, Bob only, or both Kevin and Bob? (No explanation is required. No partial credit will be given.)

(c) Explain why it is difficult for an attacker to break the RSA cryptography. (We are expecting only one sentence.)

(d) Explain why the two primes in RSA must be different. (We are expecting two reasons.)

(e) Explain why $p$ must be prime in the polynomial secret sharing with mod $p$. (We are expecting two reasons.)

**4. Stable Marriage (8 points, 3/5 points for each part)**

(a) Is the pairing {(1,A),(2,B),(3,C)} stable for the following case? Why?

| Men | Preference Lists |
|---|---|
| 1 | C > A > B |
| 2 | B > C > A |
| 3 | B > C > A |

| Women | Preference Lists |
|---|---|
| A | 2 > 1 > 3 |
| B | 3 > 1 > 2 |
| C | 3 > 2 > 1 |

(b) Find a stable pairing for the following case.

| Men | Preference Lists |
|---|---|
| 1 | D > B > A > C |
| 2 | A > D > B > C |
| 3 | D > C > B > A |
| 4 | D > A > B > C |

| Women | Preference Lists |
|---|---|
| A | 1 > 4 > 2 > 3 |
| B | 4 > 3 > 2 > 1 |
| C | 1 > 3 > 2 > 4 |
| D | 3 > 1 > 2 > 4 |

**5. Minions Using RSA (8 points, 5/3 points for each part)**

Kevin and Bob decide to apply the RSA cryptography so that Kevin can send a secret message to Bob.

(a) Assuming $p = 3$, $q = 11$, and $e = 7$, what is $d$? Calculate the exact value.

(b) Following Part (a), what is the original message if Bob receives 4? Calculate the exact value.

**6. Minions Using Error Correction Codes (10 points, 5 points for each part)**

(a) Kevin wants to send a message of 4 packets to Stuart and guard against 1 lost packet. Working over $GF(7)$, he finds the unique polynomial $P(x)$ that passes through the points he wants to send, and sends Stuart 5 packets: $(0,P(0))$, $(1,P(1))$, $(2,P(2))$, $(3,P(3))$, $(4,P(4))$. Stuart receives the following packets: $(0,3)$, $(1,0)$, $(2,0)$, $(4,0)$. What is the value of the missing packet? Calculate the exact value.

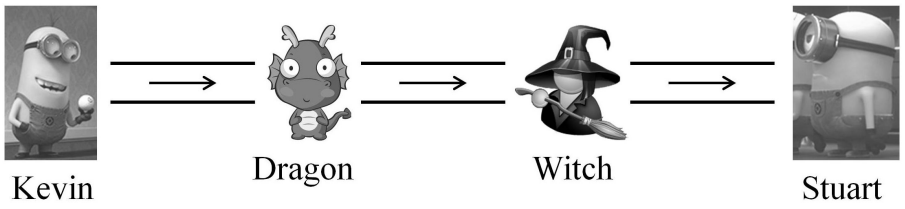


Figure 2: Minions using error correction codes [http://despicableme.wikia.com/wiki/Despicable_Me_Wiki].

(b) Kevin wants to send a message of 60 ordered packets to Stuart. Those packets will first go through a hungry dragon who will eat at most $\frac{1}{5}$ of all packets (do not ask why the dragon loves eating packets). The remaining packets will then go through a powerful but malicious witch who will change the data of at most $\frac{1}{8}$ of all packets. Given this scenario, how many packets should Kevin send so that Stuart can recover the message?

**7. TRUE or FALSE — Second Round (40 points, 10 points for each part)**

For any of the following statements, claim TRUE or FALSE first. If you claim TRUE, prove it. If you claim FALSE, disprove it (*e.g.*, provide a counterexample).

(a) $a$ is an odd number if and only if $a^2$ is an odd number.

TRUE FALSE

(b) If

$$\begin{aligned} a_0 &= 0; \\ a_1 &= 1; \\ a_n &= a_{n-1} + 2a_{n-2} + 2 \text{ for any integer } n \geq 2, \end{aligned}$$

then $a_n = 2^n - 1$ for any integer $n \geq 0$.

TRUE FALSE

(c) For all integers $a, b, c$ where $c > 0$, if $a$ has no multiplicative inverse mod $c$, then $ax \equiv b \pmod{c}$ has no solution.

TRUE FALSE

(d) Given $n$ ($n \geq 1$) integers $x_1, x_2, \ldots, x_n$ and a prime $p$,

$$(x_1 + x_2 + \ldots + x_n)^p \equiv x_1^p + x_2^p + \ldots + x_n^p \pmod{p}.$$

TRUE FALSE

**8. Simple But Not Easy (10 points)**

Prove that, for any positive integer $n$, $\left(3+\sqrt{5}\right)^n + \left(3-\sqrt{5}\right)^n$ is divisible by $2^n$.

**9. TRUE or FALSE — Ultimate and Bonus Round (15 bonus points)**

For the following statement, claim TRUE or FALSE first. If you claim TRUE, prove it. If you claim FALSE, disprove it.

For any preference lists of 3 men and 3 women, it is impossible to have 5 or more stable pairings in the stable marriage problem.

TRUE FALSE

(Extra Page: Remember to clearly tell in the space provided for a question to look here.)

(Extra Page: Remember to clearly tell in the space provided for a question to look here.)

(Extra Page: Remember to clearly tell in the space provided for a question to look here.)