Practice Midterm 1

1. A 3 by 3 table T is filled with the numbers 1 to 9 in arbitrary order, each number occurring exactly once. True or false? Justify your answer. Specify your proof method.

   (a) There exists a table T in which the sum of every column is even.

   Solution: False. We prove it by contradiction. If such a table existed the sum of all its columns would be even, so the sum of all numbers in it would be even. But the table contains five odd numbers and four even numbers so their sum is odd.

   (b) There exists a table T in which the sum of every column is odd.

   Solution: True. This table is of the desired kind:

$$\begin{array}{ccc} 1 & 3 & 5 \\ 7 & 2 & 4 \\ 9 & 6 & 8 \end{array}$$

2. A bug sits at the origin 0. In each step it can jump by 21 positions to the left or by 37 positions to the right.

   (a) Show that the bug can reach all integer positions. (**Hint:** Start with position 1.)

   Solution: As $\gcd(37, 21) = 1$ we can write 1 as $1 = s \cdot 37 + t \cdot 21$. We can simultaneously add 21 to s and subtract 37 from t without changing the equality, ensuring that s eventually becomes positive and t becomes negative. Then taking t left jumps and s right jumps is guaranteed to reach 1. Taking tn left jumps and sn right jumps is guaranteed to reach any positive n.
   When n is negative we have $-1 = -s \cdot 37 - t \cdot 21$. By adding enough 21s to $-s$ and subtracting the same number of 37s from $-t$ we ensure $-s$ is positive and $-t$ is negative so -1 can also be reached with $-s$ left jumps and $-t$ right jumps. Then any negative $-n$ can be reached with $-sn$ left jumps and $-tn$ right jumps.

   (b) How many left jumps and how many right jumps should the bug take to reach position 1?

   Solution: We write 1 and a combination of 21 and 37 using extended Euclid's algorithm:

$$\begin{aligned} E(37, 21) &= E(21, 16) & 37 &= 21 + 16 \\ &= E(16, 5) & 21 &= 16 + 5 \\ &= E(5, 1) & 16 &= 3 \cdot 5 + 1 \end{aligned}$$

   from where

$$1 = 16 - 3 \cdot 5 = 16 - 3 \cdot (21 - 16) = -3 \cdot 21 + 4 \cdot 26 = -3 \cdot 21 + 4 \cdot (37 - 21) = 4 \cdot 37 - 7 \cdot 21.$$

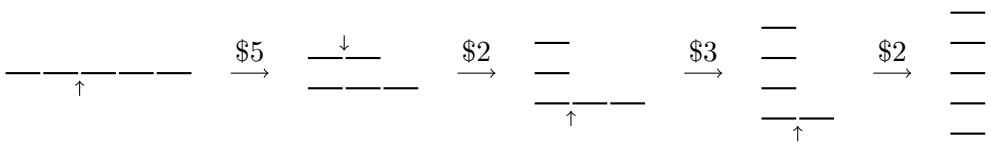
   Therefore 1 can be reached with 4 right jumps and 7 left jumps.
   We can extend this solution to provide an alternative "constructive" proof for part (a). Any positive n can be reached with $4n$ right jumps and $7n$ left jumps. For the negative numbers, we can write

$$-1 = -4 \cdot 37 + 7 \cdot 21 = (-4 + 21) \cdot 37 + (7 - 37) \cdot 21 = 17 \cdot 37 - 30 \cdot 21$$

   so -1 can be reached with 17 right jumps and 30 left jumps, and $-n$ can be reached with $17n$ right jumps and $30n$ left jumps.

3. A stick of length n is to be broken up into n unit sticks in a sequence of moves. A move consists of splitting a long stick into two shorter sticks. The cost of the move in dollars is the length of the stick being split.

   For example, here is a sequence of moves that breaks up a stick of length 5 at a cost of 12 dollars:



   (a) Use strong induction to prove: For every $n \geq 1$, the total cost of breaking up a stick of length n can be at most $\frac{1}{2}n^2 + \frac{1}{2}n - 1$ dollars, regardless of the sequence of moves.

   Base case: When $n = 1$ there is nothing to break, the cost is zero, and $\frac{1}{2} \cdot 1^2 + \frac{1}{2} \cdot 1 - 1 = 0$.

   Inductive step: Assume the claim is true for all sticks of length up to $n-1$. In the first move a length n stick is broken into parts of length a and b for some a and b that add up to n at a cost of n. By inductive assumption, the cost of breaking up the length a part is $\frac{1}{2}a^2 + \frac{1}{2}a - 1$ and the cost of breaking up the length b part is $\frac{1}{2}b^2 + \frac{1}{2}b - 1$ for a total of

$$\begin{aligned}(\tfrac{1}{2}a^2 + \tfrac{1}{2}a - 1) + (\tfrac{1}{2}b^2 + \tfrac{1}{2}b - 1) + n &= \tfrac{1}{2}(a^2 + b^2) + \tfrac{1}{2}(a+b) + n - 2 \\ &= \tfrac{1}{2}(a+b)^2 - ab + \tfrac{1}{2}(a+b) + n - 2 \\ &= \tfrac{1}{2}(a+b)^2 + \tfrac{1}{2}(a+b) - 1 + (a + b - ab - 1) \quad \text{because } n = a+b \\ &= \tfrac{1}{2}(a+b)^2 + \tfrac{1}{2}(a+b) - 1 - (a-1)(b-1).\end{aligned}$$

   As a and b are at least 1, $(a-1)(b-1)$ is nonnegative, so the cost of a length-n stick is at most $\frac{1}{2}(a+b)^2 + \frac{1}{2}(a+b) - 1 = \frac{1}{2}n^2 + \frac{1}{2}n - 1$, completing the induction.

   (b) Show that there exists a move sequence of cost $\frac{1}{2}n^2 + \frac{1}{2}n - 1$ dollars that breaks up a length n stick.

   Solution: If we keep splitting the stick into a piece of size 1 and a piece of size $n-1$ the cost is n for the first step, $n-1$ for the second step, and so on until 2 for the last step. The total cost is $n+(n-1)+\cdots+2$, which is one less than the sum of the first n numbers. It equals $n(n+1)/2 - 1 = \frac{1}{2}n^2 + \frac{1}{2}n - 1$.

4. In "baby RSA" with modulus $p = 17$, Eve intercepted the ciphertext $c = 4$. The public key is $e = 3$.

   (a) What is Bob's private key d?

   Solution: e and d are multiplicative inverses modulo $p - 1 = 16$. To find d we should solve $ed \equiv 1 \pmod{16}$. One step of extended Euclid's algorithm gives $16 = 5 \cdot 3 + 1$, so $1 = -5 \cdot 3 + 1 \cdot 16$. Therefore $e \equiv 3^{-1} \equiv -5 \equiv 11 \pmod{16}$.

   (b) What is Alice's message m?

   Solution: $m \equiv c^d = 4^{11} \pmod{17}$. Using fast multiplication,

$$4^{11} \equiv 4 \cdot (4^2)^5 \equiv 4 \cdot 16^5 \equiv 4 \cdot (-1)^5 \equiv 4 \cdot -1 \equiv -4 \equiv 13 \pmod{17}.$$

Practice Midterm 2

1. Express the sentence "Any two people who are not friends have a friend in common" using quantifiers and logical operators. Use x, y, z as variables and $F(x, y)$ for "x and y are friends."

   Solution: $\forall x, y : \text{NOT } F(x, y) \longrightarrow (\exists z : F(x, z) \text{ AND } F(z, y))$.

   Alternative solution: $\forall x, y : F(x, y) \text{ OR } (\exists z : F(x, z) \text{ AND } F(z, y))$.

2. Show that for every integer n, if $n^3 + n$ is divisible by 3 then $2n^3 + 1$ is *not* divisible by 3.

   Solution: We can prove this proposition by cases depending on the residue of $n^3 + n$ modulo 3. If $n \equiv 0 \pmod 3$ then $n^3 + n$ is divisible by 3, while $2n^3 + 1 \equiv 1 \pmod 3$, so $2n^3 + 1$ is not divisible by 3, so the proposition holds. If $n \equiv 1 \bmod 3$ then $n^3 + n \equiv 2 \pmod 3$, so $n^3 + n$ is not divisible by 3 and the proposition holds again. If $n \equiv -1 \pmod 3$, then $n^3 + n \equiv 1 \pmod 3$ and $n^3 + n$ is not divisible by 3 again.

   Alternative solution: $2n^3 + 1$ equals $(n^3 + n) + (n^3 - n) + 1$. In Lecture 3 we showed that $n^3 - n$ is divisible by 6, so also by 3. It follows that $(n^3 + n) + (n^3 - n) \equiv 0 \pmod 3$ so $2n^3 + 1 \equiv 1 \pmod 3$.

3. True or false? Justify your answer. Specify your proof method.

   (a) For all integers a, b, c, at least one of the three numbers $a + b$, $b + c$, $c + a$ is even.

   Solution: True. We prove it by contradiction. Suppose $a + b$, $b + c$, and $c + a$ are all odd. The sum of all three must then be odd. But the sum equals $2(a + b + c)$ which is an even number, a contradiction. This proof can also be formulated using modular arithmetic: Assuming $a + b \equiv 1$ and $b + c \equiv 1$ and $c + a \equiv 1$ modulo 2, adding the equations yields the conclusion

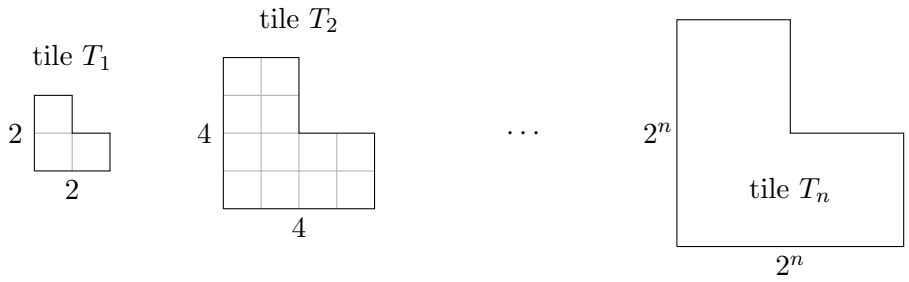
$$0 = 0a + 0b + 0c \equiv 2a + 2b + 2c \equiv 1 + 1 + 1 \equiv 1 \pmod 2$$

   which is a contradiction.

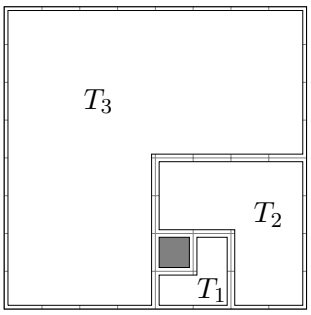
   (b) For all integers a, b, c, at least one of the three numbers $a + b$, $b + c$, $c + a$ is odd.

   Solution: False. When $a = b = c = 0$ then all three numbers are zero therefore all are even.

4. **Claim:** For every $n \geq 1$, a $2^n \times 2^n$ board with one square removed (in any position) can be filled with tiles $T_1, \ldots, T_n$ below (one of each type).



   (a) Describe a tiling for the following board ($n = 3$ with square $(5, 2)$ missing).



   (b) Prove the claim. Specify your proof method.

   Solution: We prove the claim by induction on n. In the base case $n = 1$ after removing a square the board is in the shape of a single tile so the claim holds. For the inductive step, assume the claim holds for all $2^n \times 2^n$ boards. Take a $2^{n+1} \times 2^{n+1}$ board with a square removed and divide it into four equal quadrants. By the inductive hypothesis, the quadrant containing the missing square can be tiled with tiles $T_1, \ldots, T_{n-1}$. The remaining three quadrants can be tiled with T_n.

Practice Midterm 3

1. Underline and explain the mistake in the following "proof."

   Proposition. In every group of friends there exists a person with an even number of friends.

   Proof. By induction on the number of people n. When $n = 1$ the one person has zero friends, and zero is even. Now assume it is true for groups of n people. Let G be a group of $n + 1$ people. Take out any person from G. By inductive hypothesis the remaining group G' has someone, say Alice, with an even number of friends. Since Alice is also in G, G has a person with an even number of friends. □

   Solution: If Alice has an even number of friends in G' we cannot conclude she has an even number of friends in G'. Her number of friends in G and G' may be of different parity. For example if G consists of Alice and Bob and they are friends then Alice has an odd number of friends in G but after removing Bob to obtain G', Alice is left alone and has zero (an even number) of friends.

2. For which nonzero integers n is the number $\frac{\sqrt{2}}{n} - \frac{n}{\sqrt{2}}$ rational? Justify your answer.

   Solution: It is never rational. We prove it by contradiction. Assume $\sqrt{2}/n - n/\sqrt{2} = p/q$ for some integers p and $q \neq 0$. Simplifying we obtain $(2 - n^2)/\sqrt{2}n = p/q$. If p equals zero than $2 - n^2$ must also equal zero, so n must equal $\sqrt{2}$ or $-\sqrt{2}$. Both of these numbers are irrational by Theorem 1. If p is not zero, we can write $\sqrt{2} = (2 - n^2)q/p$ which is a ratio of integers with nonzero denominator. This contradicts Theorem 1 again.

3. Alice has infinitely many \$6, \$10, and \$15 stamps.

   (a) Can she make all integer postages of \$30 and above?

   Solution: Alice can make all integer postages from \$30 to \$35 as follows:

   $$\begin{aligned} \$30 &= 5 \times \$6 \\ \$31 &= \$6 + \$10 + \$15 \\ \$32 &= 2 \times \$6 + 2 \times \$10 \\ \$33 &= 3 \times \$6 + \$15 \\ \$34 &= 4 \times \$6 + \$10 \\ \$35 &= 2 \times \$10 + \$15 \end{aligned}$$

   Now we show that she can make any amount n above 30 by strong induction on n. We already covered the cases $30 \leq n \leq 35$. Now assume that $n > 35$ and she can make all amounts between \$30 and \$$n$. Then $n - 6 \geq 30$ and by inductive assumption she can make $n - 6$ dollars. By adding one \$6 stamp she obtains n dollars.

   (b) What if the \$10 stamp was replaced by a \$9 stamp?

   Solution: No. She cannot make 31 dollars. The postage amounts are combinations of 6, 9, and 15. As 3 divides all it will divide any such combination. However 3 does not divide 31.

4. Bob has 32 *b*lue, 33 *r*ed, and 34 *g*reen balls. At every turn he takes out two balls and replaces them with two different balls by the following replacement rule:

   $$bg \to rr \quad gr \to bb \quad rb \to gg \quad rr \to bg \quad bb \to gr \quad gg \to rb.$$

   (a) Formulate this game as a state machine. Describe the states, start state, and transitions mathematically.

   Solution: the states are triples (B, R, G) indicating the number of balls of each color. The start state is $(32, 33, 34)$. The transitions are from (B, R, G) to the states $(B-1, R-1, G+2)$, $(B+2, R-1, G-1)$, $(B-1, R-1, G+2)$, $(B+1, R-2, G+1)$, $(B-2, R+1, G+1)$, $(B+1, R+1, G-2)$ as long as all numbers remain non-negative.

(b) Can Bob obtain 99 balls of the same color? Justify your answer.
(**Hint:** Look at the difference between the number of red and blue balls.)

Solution: The predicate "$R - B \equiv 1 \pmod 3$" is an invariant. It holds in the start state and it is preserved by all transitions as $R - B$ can only change by -3, 0, or 3. If all 99 balls are of the same color then 3 divides $R - B$, so that state cannot be reached.

Practice Midterm 4

1. Are the propositions "Every two people have a common friend" and "Every person has at least two friends" logically equivalent? Justify your answer.

   Solution: They are not logically equivalent. Suppose the world consists of Alice, Bob, Charlie, and Dave, and the following friendships: Alice with Bob, Bob with Charlie, Charlie with Dave, Dave with Alice. Then every person has two friends, but Alice and Bob have no common friend.

2. Show that for every positive real number x, at least one of the numbers $\sqrt{x} + 1$ and $\sqrt{2} \cdot x$ is irrational.

   Solution: For contradiction suppose they are both rational. Then $x = ((\sqrt{x} + 1) - 1)^2$ is also rational. As it is positive, $(\sqrt{2} \cdot x)/x$ is the ratio of two rational numbers with nonzero denominator so it is rational. But this equals $\sqrt{2}$, contradicting its irrationality.

3. Bob is waiting for a secret message from Alice. He publishes RSA modulus $n = 21$ and public key $e = 5$.

   (a) Alice's message is $m = 8$. What is the ciphertext that she sends out? Show your calculations.

   Solution: The ciphertext is $m^e \bmod n$, namely

   $$8^5 \equiv 8 \cdot 8^4 \equiv 8 \cdot 64^2 \equiv 8 \cdot 1^2 = 8 \pmod{21}$$

   because $64 = 3 \cdot 21 + 1 \equiv 1 \pmod{21}$.

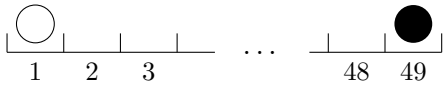
   (b) Alice sends another ciphertext $c = 2$ and this one is intercepted by Eve. What was Alice's message?

   Solution: As n is the product of the two primes $p = 3$ and $q = 7$, Eve can recover the decryption key by solving for $ed \equiv 1 \pmod{(p-1)(q-1)}$, namely $5d \equiv 1 \pmod{12}$. Extended Euclid's algorithm gives

   $$\begin{aligned} E(12,5) &= E(5,2) & 12 &= 2 \cdot 5 + 2 \\ &= E(2,1) & 5 &= 2 \cdot 2 + 1 \end{aligned}$$

   from where $1 = 5 - 2 \cdot 2 = 5 - 2 \cdot (12 - 2 \cdot 5) = -2 \cdot 12 + 5 \cdot 5$, so d equals 5. The ciphertext decrypts to $c^d \bmod n$, which equals $2^5 = 32 \equiv 11 \pmod{21}$. Alice's message was 11.

4. A long ledge is divided into slots numbered from 1 to 49.

   A white ball and a black ball are placed in the first and last slot, respectively. In every step one of the balls is moved 5 slots to the left *or* 10 slots to the right of its current position.

   (a) Formulate this process as a state machine. Describe the states, start state, and transitions.

   Solution: The states are ordered pairs of numbers (w, b) between 1 and 49 describing the white and black ball's slot respectively. The start state is $(1, 49)$. The transitions are

   $$(w, b) \to (w - 5, b) \text{ OR } (w + 10, b) \text{ OR } (w, b - 5) \text{ OR } (w, b + 10).$$

(b) *Invariant:* The slot numbers of the black and white balls differ by $\underline{3}$ modulo $\underline{5}$.
Fill in the blanks and provide a proof of invariance.

Solution: In the start state, $49 - 1 = 48 \equiv 3 \pmod 5$ so the invariant holds. Now assume $b - w \equiv 3 \pmod 5$ in a given state. The transitions change the value of $b-w$ by $+5$, -10, -5, and -10 respectively. As all these numbers are 0 modulo 5 the value $b - w \pmod 5$ remains the same.

(c) Can the two balls ever occupy adjacent slots? Justify your answer.

Solution: No. If the balls occupy adjacent slots then $b - w$ equals to 1 or -1, that is 1 or 4 modulo 5. The invariant is not satisfied so such a state can never be reached.