Practice Midterm 1

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

3. Prove that for every integer n there exists an integer k such that $|n^2 - 5k| \leq 1$. (**Hint:** What is n^2 mod 5?)

   Solution: First we check that for all n, n^2 mod 5 equals 0, 1 or 4:

n mod 5	0	1	2	3	4
n^2 mod 5	0	1	4	4	1

   Since $4 \equiv -1 \pmod 5$ it follows that for every n, n^2 is congruent to 0, 1, or -1 modulo 5. Therefore n^2 is of the form $5k$ or $5k - 1$ or $5k + 1$ for some integer k. In all cases $|n^2 - 5k| \leq 1$.

4. The numbers `12345678` are listed in order. In each step you can take three consecutive numbers abc and reorder them as cab, for example `25431687` $\rightarrow$ `25438167`. Can you ever obtain `81234567`?

   Solution: No. We show that the "number of inversions in the list is even" is an invariant. (An inversion is a pair of numbers that are out of order.) As the list `81234567` has seven inversions (`81` to `87`) it can never be reached.

   In the start state `12345678` there are no inversions so the invariant holds. Now assume some list ℓ has i inversions. After reordering abc as cab the number of inversions can increase by 2 (if c was greater than both a and b), decrease by 2 (if c was smaller than both), or stay the same (if it was in between the two). Therefore the number of inversions stays even so the invariant is preserved by all transitions.

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. Can 4 be expressed as an integer linear combination of 47 and 13? If no, provide a proof. If yes, give such a combination and explain how you obtained it.

   Solution: Yes. We will show that the GCD of 47 and 13 is 1 by executing Euclid's algorithm. By Theorem 3, 1 is a combination of 47 and 13. Multiplying both side of this combination by 4 we can obtain 4 as a combination of 47 and 13.

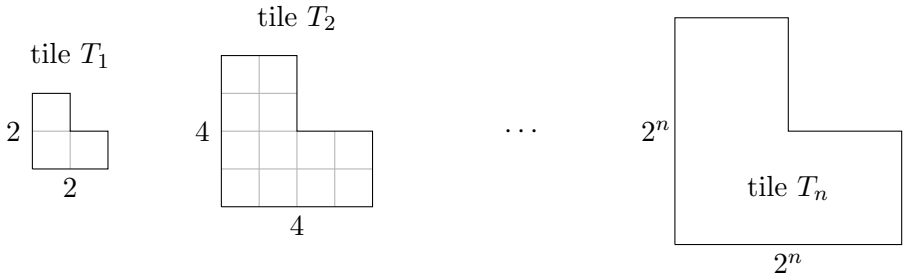
$$\begin{aligned} E(47, 13) &= E(13, 8) && \text{because } 47 = 3 \cdot 13 + 8 \\ &= E(8, 5) && \text{because } 13 = 8 + 5 \\ &= E(5, 3) && \text{because } 8 = 5 + 3 \\ &= E(3, 2) && \text{because } 5 = 3 + 2 \\ &= E(2, 1) && \text{because } 3 = 2 + 1 \\ &= E(1, 0) && \text{because } 2 = 2 \cdot 1 \\ &= 1. \end{aligned}$$

   To find the coefficients it is sufficient to express 2 as a combination of the two numbers. We work backwards from $5 = 3 + 2$:

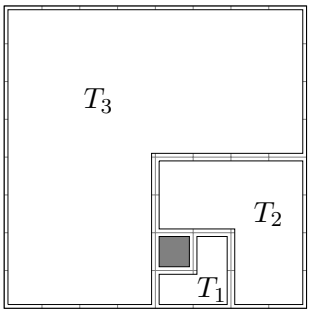
$$\begin{aligned} 2 &= 5 - 3 \\ &= 5 - (8 - 5) = -8 + 2 \cdot 5 \\ &= -8 + 2 \cdot (13 - 8) = 2 \cdot 13 - 3 \cdot 8 \\ &= 2 \cdot 13 - 3 \cdot (47 - 3 \cdot 13) \\ &= -3 \cdot 47 + 11 \cdot 13. \end{aligned}$$

   Doubling both sides we get $4 = -6 \cdot 47 + 22 \cdot 13$.

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."

   Theorem. 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. Prove that for every positive integer n, $\gcd(n^2 + n + 1, n + 1) = 1$.
   (**Hint:** Use the connection between gcd and combinations.)

   Solution: 1 is an integer combination of the two numbers: $1 = 1 \cdot (n^2 + n + 1) - n \cdot (n + 1)$. As the GCD must divide all integer combinations it must equal one.

3. 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.

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. Is the following deduction rule valid?

$$\frac{\forall x \exists y\colon P(x,y) \qquad \exists x \forall y\colon P(x,y)}{\forall x \forall y\colon P(x,y)}$$

Solution: No. Suppose $P(x,y)$ means "person x is happy on day y", Alice is happy on Monday, Alice is happy on Tuesday, Bob is happy on Monday, but Bob is not happy on Tuesday. Then $\forall x \exists y\colon P(x,y)$ is true because everyone is happy sometimes – on Monday, $\exists x \forall y\colon P(x,y)$ is true because someone (Alice) is happy all the time, but $\forall x \forall y\colon P(x,y)$ is false because Bob is unhappy on Tuesday, so not everyone is happy all the time.

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 has received from Alice the RSA ciphertext $c = 2$. The modulus is $n = pq$ with $p = 3$ and $q = 5$. The encryption key is $e = 3$.

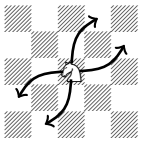
   (a) Calculate Bob's decryption key d.

   Solution: e and d must satisfy the equation $ed \equiv 1 \pmod{(p-1)(q-1)}$, so $3d \equiv 1 \pmod 8$. Therefore d is the multilpicative inverse of 3 modulo 8. We find it using extended Euclid's algorithm: $8 = 2\cdot 3 + 2$ and $3 = 2 + 1$, so $1 = 3 - 2 = 3 - (8 - 2\cdot 3) = -8 + 3\cdot 3$. Therefore $d = 3$.

   (b) Decrypt Alice's message m.

   Solution: The decrypted message is $c^d = 2^3 = 8 \pmod{15}$.
   (You can verify that $m^e = 8^3 \equiv 2 = c \pmod{15}$.)

4. A knight jumps around an infinite chessboard. Owing to injury it can only make these four moves:



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

   Solution: The states are integer pairs (x,y). The start state is $(0,0)$. The transitions out of (x,y) are

$$(x,y) \to (x-2,y-1) \quad \text{or} \quad (x-1,y-2) \quad \text{or} \quad (x+2,y+1) \quad \text{or} \quad (x+1,y+2).$$

   (b) Can the knight ever reach the square immediately to the left of its initial one?

   Solution: No. The predicate "3 divides $x+y$" is an invariant of this state machine. It holds initially, and after every transition $(x,y) \to (x',y')$ we have $x'+y' = x+y-3$ in the first two cases and $x'+y' = x+y+3$ in the other two. Assuming the invariant holds before the transition (i.e., 3 divides $x+y$) it also holds after the transition (3 divides $x'+y'$).
   The invariant does not hold for state $(-1,0)$ so that state cannot be reached.