Harvard University
Computer Science 20

Problem Set 3

PROBLEM 1

The sum of the digits of a positive integer number is divisible by 9 if and only if the number is divisible by 9. (So 234 and 567 are both divisible by 9.) Prove this statement, by writing it in terms of modular arithmetic. Hint: think of an n-digit number as a sequence of digits $d_n d_{n-1} \ldots d_2 d_1$. Can you write that number in terms of it digits in a useful way?

Solution.
I will prove that the sum of the digits of a number is evenly divisible by 9 if and only if the number is also divisible by 9 through chains of equivalences which will show that the left hand and right hand side are equivalent to oneanother. In other words, given a number which can be represented as an enumerated sequence of its digits d_i with a length of n, I will prove $\sum_{i=0}^{n-1} d_i \equiv_9 0 \iff \sum_{i=0}^{n-1} 10^i d_i \equiv_9 0$.

Lemma1. $\forall k \in \mathbb{Z}^+ . 10^k \in [1]_9$
$10^n = 1 + \sum_{i=0}^{n-1} 10^i 9$
$(10^n) \mod 9 = (1 + \sum_{i=0}^{n-1} 10^i 9) \mod 9$
$\sum_{i=0}^{n-1} 10^i 9 = 9k; k \in \mathbb{Z} \because$ the summation is just a repeated addition (multiple) of 9
$10^n \mod 9 = 9k + 1 \mod 9$
$10^n \mod 9 = 1$

$\sum_{i=0}^{n-1} 10^i d_i \equiv_9 0 \iff \sum_{i=0}^{n-1} d_i \equiv_9 0$
10^i can be replaced with the equivalent expression $((\sum_{k=0}^{i-1} 10^k 9) + 1)$
$\sum_{i=0}^{n-1} (\sum_{k=0}^{i-1} (10^k 9) + 1) d_i \equiv_9 0 \iff \sum_{i=0}^{n-1} d_i \equiv_9 0$
$\sum_{i=0}^{n-1} (d_i \sum_{k=0}^{i-1} (10^k 9) + d_i) \equiv_9 0 \iff \sum_{i=0}^{n-1} d_i \equiv_9 0$
$\sum_{i=0}^{n-1} (d_i \sum_{k=0}^{i-1} (10^k 9)) + \sum_{i=0}^{n-1} d_i \equiv_9 0 \iff \sum_{i=0}^{n-1} d_i \equiv_9 0$
$[\sum_{i=0}^{n-1} (d_i \sum_{k=0}^{i-1} 10^k 9) \mod 9 + \sum_{i=0}^{n-1} d_i \mod 9] \mod 9 = 0 \iff \sum_{i=0}^{n-1} d_i \equiv_9 0$
The summations of $10^k 9$ which occurs on the left hand side can be simplified to $9n$ where $n \in \mathbb{Z}$ because it is just a repeating sum of '9'.
$[n9 \mod 9 + \sum_{i=0}^{n-1} d_i \mod 9] = 0 \iff \sum_{i=0}^{n-1} d_i \equiv_9 0$
$[0 + \sum_{i=0}^{n-1} d_i \mod 9] = 0 \iff \sum_{i=0}^{n-1} d_i \equiv_9 0$
$\sum_{i=0}^{n-1} d_i \equiv_9 0 \iff \sum_{i=0}^{n-1} d_i \equiv_9 0$

In conclusion, the sum of the digits of a number are divisible by 9 if and only if the number is also divisible by 9, because through chains of equivalences on a numerical representation of the claim the propositions where shown to be equivalent. QED.

PROBLEM 2

Use modular arithmetic to prove that the square of any integer is of the form $3k$ or $3k + 1$.

Solution.
$\mathbb{Z}_3 = \{[0], [1], [2]\}$
I will prove the claim with 3 cases: when an integer squared is in the forms 3k, 3k+1, or 3k+2

Case 1:
let $n, k, m \in \mathbb{Z}$
$n \equiv_3 0$
$n = 3k$: definition of modulus
$n^2 = 9k^2$
$3 * 3k^2 \mod 3 = 3m \mod 3$
$0 = 0$
Through chains of equivalences, both sides turn out equivalent.

Case 2:
let $n, k_1, k_2 m \in \mathbb{Z}$
$n \equiv_3 1$
$n = 3k + 1$: definition of modulus
$n^2 = 9k_1^2 + 6k_1 + 1$
$3(3k_1^2 + 2k_1) + 1 \mod 3 = 3m + 1 \mod 3$
let $k_2 := (3k_1^2 + 2k_1)$ $3k_2 + 1 \mod 3 = 3m + 1 \mod 3$ $1 = 1$
Through chains of equivalences, both sides turn out equivalent.

Case 3:
let $n, k_1, k_2 m \in \mathbb{Z}$
$n \equiv_3 2$
$n = 3k + 2$: definition of modulus
$n^2 = 9k_1^2 + 12k_1 + 4$
$3(3k_1^2 + 4k_1 + 1) + 1 \mod 3 = 3m + 2 \mod 3$
let $k_2 := (3k_1^2 + 4k_1 + 1)$ $3k_2 + 1 \mod 3 = 3m + 2 \mod 3$ $1 \neq 2$
Through chains of equivalences, both turn out in-equal.

In conclusion, by splitting the domain of integers into groupings/classes ([0], [1], [2]) we can test each as cases through chains of equivalences. After testing each case, it was determined that squared integers could only be represented in the forms 3k or 3k+1 where k is an integer. QED.

PROBLEM 3

When is $|P(A \cup B)| = |P(A)| \cdot |P(B)|$? Give a case when they are not equal. Determine an expression for the ratio $\frac{|P(A \cup B)|}{|P(A)| \cdot |P(B)|}$ and explain why it is correct.

Solution.
$\sum_{k=0}^{n} \binom{n}{k} = 2^n$
The cardinality of a powerset of a set is equal to 2^n where n is the number of elements in the set. Therefore the original equation can be rewritten as $2^{A \cup B} = 2^{|A|} * 2^{|B|}$ or $2^{|A \cup B|} = 2^{|A|+|B|}$ or $|A \cup B| = |A| + |B|$ $|P(A \cup B)| = |P(A)| \cdot |P(B)|$ can be expected to hold true when $|A \cup B| = |A| + |B|$.

A case when they $|P(A \cup B)|$ would not equal $|P(A)| \cdot |P(B)|$ would be when $A := 1, 2$ and $B := 1, 4$ such that $|P(A)| = 4; |P(B)| = 4; |P(A \cup B)| = 8; |P(A)| * |P(B)| = 16$
$\frac{|P(A \cup B)|}{|P(A)| \cdot |P(B)|}$
$\frac{2^{|A \cup B|}}{2^{|A|+|B|}}$: replace $|P(A \cup B)|$ and $|P(A)| \cdot |P(B)|$ with alternative forms determined above
$2^{|A \cup B|-|A|-|B|}$: exponent rules

$\frac{|P(A \cup B)|}{|P(A)| \cdot |P(B)|} = 2^{|A \cup B|-|A|-|B|}$ the ratio represents the how the number of elements in the union of A and B differs from the total count of elements in A and B if there were no overlap.

PROBLEM 4

Is it always true that for two (finite) sets A and B that $(A - B) \cap (B - A) = \emptyset$? Prove it or give a counterexample.

Solution.
I will prove that for any two finite sets A and B that $(A - B) \cap (B - A) = \emptyset$, by re-expressing $(A - B) \cap (B - A) = \emptyset$ through chains of equivalences until it is equivalent to $\emptyset$

$(A - B) \cap (B - A) = \emptyset$
$(A \cap \bar{B}) \cap (B \cap \bar{A}) = \emptyset \because A - B = A \cap \bar{B}$
$(A \cap \bar{A}) \cap (B \cap \bar{A}) = \emptyset$: associative property
$\emptyset \cap \emptyset = \emptyset$: $S \cap \bar{S}$ is null because it is the intersection of a set and its complement (everything but the contents of the set)

In conclusion, It is true that for two finite sets A and B that $(A - B) \cap (B - A) = \emptyset$, because after expressing sufficient chains of equivalences $(A \cap \bar{A}) \cap (B \cap \bar{A}) = \emptyset$ is achieved. Here, you take the intersection of A and $\bar{A}$ ie everything in A and everything not it A: which will always result in a null set. Proving that $(A - B) \cap (B - A)$ is equivalent to $\emptyset$. QED.

PROBLEM 5

Let $g : \mathbb{Z} \to \mathbb{Z}$ be an injective function. Define $f : (\mathbb{Z} \times \mathbb{Z}) \to (\mathbb{Z} \times \mathbb{Z})$ such that $f(x, y) = (g(x) + g(y), g(x) - g(y))$. Prove that f is also injective.

Solution.
Injective function definition: $\forall a, b \in A.(f(a) = f(b)) \to (a = b)$ where A is function f's domain
We will need to prove that $\forall x_1, y_1, x_2, y_1 \in \mathbb{Z}.[f(x_1, y_1) = f(x_2, y_2)] \to [x_1 = x_2 \wedge y_1 = y_2]$

let $x_1, y_1, x_2, y_1 \in \mathbb{Z}$
The function f can be split into two separate functions/relations. According to our multivariate interpretation of hte injective function definition, the following must be true.
$g(x_1) + g(y_1) = g(x_2) + g(y_2)$
$g(x_1) - g(y_1) = g(x_2) - g(y_2)$

If we add the equivalences, we can isolate and compare g(x)
$(g(x_1) + g(y_1)) + (g(x_1) - g(y_1)) = (g(x_2) + g(y_2)) + (g(x_2) - g(y_2))$
$2g(x_1) = 2g(x_2)$
$g(x_1) = g(x_2)$
since g(x) is injective (meaning each output will only have 1 unique input), we can disregard with $g(x_1) = g(x_2)$ impying $x_1 = x_2$

If we add the equivalences, we can isolate and compare g(y) $(g(x_1) + g(y_1)) - (g(x_1) - g(y_1)) = (g(x_2) + g(y_2)) - (g(x_2) - g(y_2))$
$2g(y_1) = 2g(y_2)$
$g(y_1) = g(y_2)$
since g(y) is injective (meaning each output will only have 1 unique input), we can disregard with $g(y_1) = g(y_2)$ impying $y_1 = y_2$

By manipulating our function with chains of equivalences, and making use of f's composition of the known injective function g(x), we were able to compare the inputs and check whether or not the same output can result from two diferent inputs. QED.