Harvard University
Computer Science 20

Problem Set 2

Due Thursday, February 11, 2021 at 11:59pm

SELF CHECK

- Did you clearly state the claim at the beginning of your proof?
- Did you clearly conclude your proof with a statement of what you have proved?
- Is each assertion either a given fact, a hypothesis, a definition, or a logical conclusion from prior statements?
- Are all of your variables properly introduced and quantified? Is the domain of variables clearly specified?
- Does your proof proceed logically from claim to conclusion?
- Have you removed any extraneous information or tangents that were part of your exploratory work?
- Have you considered corner cases? If you are dividing your proof into cases, have you exhausted all cases?

PROBLEM 1

If x and y are integers and $x^2 + y^2$ is even, prove that x + y is even.

Claim: $x + y$ is even, given x and y are integers and $x^2 + y^2$ is even.

Proof: Given x and y are integers and $x^2 + y^2$ is even,

then $x^2 + y^2 = (x+ y)^2$

furthermore $(x+ y)^2 = x^2 + y^2 + 2xy$

Since any even or odd number multiplied by 2 is even *(fact)*, then 2xy is even.

Thus, being a sum of three even integers, $x^2 + y^2 + 2xy$, $(x+y)^2$ is even.

Since, $(x+y)^2$ is even, then $(x+y)^2 = 2k$ for some integer k. *(Introduced variable, k)*

Furthermore, $2 \mid 2k$, therefore $2 \mid (x+y)^2$

$$2 \mid (x+y)^2 = 2 \mid (x+y)(x+y)$$

(Prime numbers have the property that if they divide a product, they must divide one or the other factor contributing to the product.

Let p = any prime number. If $p \mid cd$, then either $p \mid c$ or $p \mid d$)

Since $(x+y)(x+y)$ is being divided by a prime number, 2, either factor $(x+y)$ or $(x+y)$ is divisible by 2.

In conclusion, since either $(x+y)$ or $(x+y)$ is divisible by 2, then x+y is even.

PROBLEM 2

Prove or disprove: If 12 | x^2, then 12 | x

Claim: If 12 | x^2, then 12 | x

Disproof: A counter-example to disprove this claim is to let $x^2 = 36$.

If $x^2 = 36$, then x = + 6 or – 6.

12 | x^2 = 12 | 36, which = 12 * 3 = 36 and is valid.

12 | x = 12 | 6 = 12 | -6 = non-integer, which is invalid.

(Dividend < Divisor)

In conclusion, if 12 | x^2, then it is not necessarily true that 12 | x.

PROBLEM 3

The integers a and b are relatively prime if GCD(a,b) = 1. Prove the following claim:

Claim: If ax ≡ 1 (mod b) for some x ∈ Z, then a and b are relatively prime.

Proof: In number theory, two integers a and b are relatively prime or coprime if there is no integer > 1 that divides them both, which means that their CGD(a,b) = 1

Suppose ax ≡ 1 (mod b) for some x ∈ Z, then ax = 1+nb for some integer n.

1 is a common divisor since 1 | a and 1 | b.

Let d be any other common divisor and we want to show that d ≤ 1.

Since d | a and d | b, there are integers p and q, such that d p = a and d q = b.

Thus, ax = 1+nb

ax – nb = 1

dpx – ndq = 1

d(px – nq) = 1

Since d * some integer = 1, therefore d | 1.

If any divisor divides a dividend, it means that the dividend ≤ divisor.

Since d | 1 , then d ≤ 1

In conclusion, since any common divisor of a and b is ≤ 1, then the GCD(a, b) = 1.

Since the GCD(a, b) = 1, then then a and b are relatively prime.