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.

<u>Claim</u>: If x and y are integers and $x^2 + y^2$ is even, then x + y is even.

<u>Proof</u>:

Suppose for the contrapositive that x + y is not even.

Therefore, x + y is odd.

So, there is an integer k such that $x + y = 2k + 1$

Therefore, $(x + y)^2 = 4k^2 + 4k + 1$ and this is equal to $2(2k^2 + 2k) + 1$

But that means $(x + y)^2 = 2m + 1$, where m is the integer $(2k^2 + 2k)$

By definition this shows that $(x + y)^2$ is odd.

Hence, $(x + y)^2$ is not even.

We have therefore shown that if x + y is not even, then $(x + y)^2$ is not even.

This is the contrapositive of the claim that if $(x + y)^2$ is even, then x + y is even.

In conclusion, if x and y are integers and $x^2 + y^2$ is even, 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 x = -6

12 | x^2 would be 12 | 36, which equals 3 and is therefore valid.

12 | x would be 12 | 6 and 12 | -6

In either case the Dividend ≤ Divisor (for + divisors).

The result will be a non-integer and is therefore invalid.

In conclusion, if 12 | x^2, then 12 | x is not true for all cases.

PROBLEM 3

The integers a and b are relatively prime if GCD(a,b) = 1.

Prove the following claim:

<u>Claim</u>: If $ax \equiv 1 \pmod{b}$ for some $x \in Z$, then a and b are relatively prime.

<u>Proof</u>:

In number theory, two integers a and b are relatively prime or coprime if there is no integer > 1 that divides them both.

This means that their CGD(a,b) = 1

Suppose $ax \equiv 1 \pmod{b}$ for some $x \in Z$, then $ax = 1 + nb$ for some integer n

1 is a common divisor since $1 \mid a$ and $1 \mid b$

Let d be any other common divisor and we want to show that $d \leq 1$

Since $d \mid a$ and $d \mid b$, there are integers p and q, such that $dp = a$ and $dq = b$

Thus, $ax = 1+nb$

$$ax - nb = 1$$

$$dpx - ndq = 1$$

$$d(px - nq) = 1$$

Since $d(px - nq) = 1$, where $(px - nq)$ = any positive integer, therefore $d \mid 1$

If any divisor divides a dividend, it means that the dividend $\leq$ divisor

Since $d \mid 1$, then $d \leq 1$

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.