CSCA67

ASSIGNMENT #1 PROOFS

UNIVERSITY OF TORONTO SCARBOROUGH

XiangQian "Richard" Hong
Student Number:1005456178
October 15th

1. $\forall a \in \mathbb{Z}, \forall b \in \mathbb{Z}, \forall c \in \mathbb{Z}, (a|b) \wedge (a \not| c) \rightarrow a \not|(b+c)$

   Assume the Contrapositive: $\exists a \in \mathbb{Z}, \exists b \in \mathbb{Z}, \exists c \in \mathbb{Z}, \ni: a|(b+c) \rightarrow (a \not| b) \vee (a|c)$

$$a|(b+c) \rightarrow \frac{b+c}{a} = k, k \in Z$$
$$\frac{b+c}{a} = k, k \in Z \text{ means that } b+c \text{ must be a multiple of } a$$
$$\exists x, y \in \mathbb{Z}, \ni: b = ax, c = ay$$
$$\frac{ax+ay}{a} = \frac{ax}{a} + \frac{ay}{a}$$
$$\frac{c}{a} = \frac{ay}{a} = y, y \in \mathbb{Z} \rightarrow \frac{c}{a} \in \mathbb{Z}$$
$$\frac{c}{a} \in \mathbb{Z} \rightarrow (a|c)$$
$$\therefore \forall a \in \mathbb{Z}, \forall b \in \mathbb{Z}, \forall c \in \mathbb{Z}, (a|b) \wedge (a \not| c) \rightarrow a \not|(b+c)$$

2. Prove that the number $log_7 2$ is irrational

   Assume the contrary: $log_7 2 \in \mathbb{Q}$

$$\log_7 2 \in \mathbb{Q} \rightarrow log_7 2 = \frac{m}{n} \ni: \{m, n\} \in \mathbb{Z}, gcd(m, n) = 1, n \neq 1$$
$$log_7 2 = \frac{m}{n} \rightarrow 7^{\frac{m}{n}} = 2$$
$$7^m = 2^n$$

Lemma: Product of even integers is even and product of odd integers is odd.

$$\forall \{m, n\} \in 2\mathbb{Z} \rightarrow m \cdot n \in 2\mathbb{Z}$$
$$\{k, k_o\} \in \mathbb{Z}, m = 2k \wedge n = 2k_o \rightarrow m \cdot n \in 2\mathbb{Z}$$
$$2k \cdot 2k_o = 4kk_o = 2(2kk_o), \{k, k_o\} \in \mathbb{Z}$$

Since 2 times any integer results in an even integer,

$$\therefore \forall \{m, n\} \in 2\mathbb{Z} \rightarrow m \cdot n \in 2\mathbb{Z}$$

$$\forall \{x, y\} \in 2\mathbb{Z}+1 \rightarrow x \cdot y \in 2\mathbb{Z}+1$$
$$\{z.z_o\} \in \mathbb{Z}, x = 2z+1 \wedge y = 2z_o+1 \rightarrow x \cdot y \in 2\mathbb{Z}+1$$
$$(2z+1)(2z_o+1) = 4zz_o + 2z + 2z_o + 1 = 2(2zz_o + z + z_o) + 1$$

Since the sum of 1 and any even integer results in an odd integer,

$$\therefore \forall \{x, y\} \in 2\mathbb{Z}+1 \rightarrow x \cdot y \in 2\mathbb{Z}+1$$

Since we know that 7 is an odd integer, 2 is an even integer, and the product of even integers is even and product of odd integers is odd by **lemma**.

$$\text{Negative case: } \forall m, n < 0, \frac{1}{7^m} \neq \frac{1}{2^n}$$
$$\forall \{m, n\} \in \mathbb{Z}, n \neq 0, 7^m \neq 2^n \text{ contradicting our assumption.}$$
$$\therefore log_7 2 \in \mathbb{I} \text{ by contradiction.}$$

3. Prove facts about numbers divisable by 9

   (a) Prove that $10^n - 1$ is divisable by 9
   Base case: show $n = 0$

   $$10^0 - 1 = 0 \to 9|10^0 - 1$$

   $\therefore$ the base case holds for n = 0.
   Inductive Hypothesis: assume for some arbitrary k that $10^k - 1$ is divisible by 9.
   $10^k - 1 = 9z, z \in \mathbb{Z}$
   $10^k = 9z + 1$
   Inductive step: Prove $9|10^k - 1 \to |10^{k+1} - 1$

   $$10^{k+1} - 1 = 10^k \cdot 10^1 - 1$$
   $$10^{k+1} - 1 = (9z + 1) \cdot 10^1 - 1 \text{ by Inductive Hypothesis}$$
   $$10^{k+1} - 1 = 90z + 10 - 1$$
   $$10^{k+1} - 1 = 90z + 9$$
   $$10^{k+1} - 1 = 9(10z + 1)$$

   $(10z + 1)$ is an integer by closure, and 9 times any integer is divisible by 9.
   Since the statement holds for n = 0 and $n = k \to n = k + 1$ is also true,

   $$\therefore \forall n \in \mathbb{N}, 9|10^n - 1$$

   (b) Given a number x in decimal representation, let s represent the sum of the digits of x. Prove that $x - s$ is divisible by 9.

   $$x_i = d_0 \cdot 10^0 + d_1 \cdot 10^1 \cdots + d_i \cdot 10^i$$
   $$s_i = d_0 + d_1 + d_2 \cdots + d_i$$
   $$x_i - s_i = d_0 \cdot 10^0 - d_0 + d_1 \cdot 10^1 \cdots - d_1 + d_i \cdot 10^i - d_i$$
   $$x_i - s_i = d_0(10^0 - 1) + d_1(10^1 - 1) \cdots + d_i(10^i - 1)$$
   $$d \text{ must satisfy } 0 \leq d \leq 9$$

   In 3 (a). we have already proved that $10^n - 1$ is divisible by 9 for all natural numbers.
   Since we know that d is any integer between 0 and 9, $d(10^n - 1)$ must be divisible by 9 for all n, which means all the elements in $x_i - s_i$ must be divsible by 9.
   Finally if 9 divides every element in a set, 9 must divide the sum of that set.
   $\therefore 9|x_i - s_i = d_0(10^0 - 1) + d_1(10^1 - 1) \cdots + d_i(10^i - 1)$

4. Let p be a prime number and consider the set of numbers $S = 1, 2, \ldots, p-1$. Let $a \in S$. Prove the following two claims:

   (a) no two numbers from the list $1 \cdot a, 2 \cdot a, \ldots, (p-2) \cdot a, (p-1) \cdot a$ are congruent modulo p

   Assume the contrary; there are two numbers from the list that are congruent modulo p.

   If they are congruent mod p, then they must share the same remainder.

   $\exists x, y, a \in S$

   $x \cdot a = pk_1 + r$

   $y \cdot a = pk_2 + r$

   $k_1, k_2 \in \mathbb{Z}$

   $x \cdot a - y \cdot a = pk_1 + r - pk_2 + r$

   $a(x-y) = p(k_1 - k_2)$

   $a(x-y) = p(k_1 - k_2)$ implies that $a \cdot (x-y)$ is equal to some multiple of the prime p

   by the Fundamental Theorem of Arithmetic: if $a \cdot (x-y) = kp, k = \mathbb{Z} \Rightarrow a = p \vee (x-y) = p$

   Contradiction:

   since S is bounded by $(p-1)$, $\forall a \in S, a \leq (p-1) \Rightarrow a \neq p$.

   since $x, y \in S, (x-y) < (p-1) \Rightarrow p(x-y) < p$

   as neither a, $(x-y)$ can equal to p:

   $\therefore$ no two numbers from $1 \cdot a, 2 \cdot a, \ldots, (p-2) \cdot a, (p-1) \cdot a$ are congruent modulo p by contradiction

   QED

   (b) Prove that there exists $b \in S$ such that $b \cdot a \equiv_p 1$.

   $\exists b, a \in S, \ni: b \cdot a \equiv_p 1$

   Identity $a < b \Rightarrow a \bmod b = a$

   $1 \bmod p = 1$

   $b \cdot a = 1 \Rightarrow (b \cdot a) \bmod p = 1$

   $b \cdot a = 1, b = 1, a = 1$

   $\therefore \exists b, a \in S, \ni: b \cdot a \equiv_p 1$

   QED

5. Use the pigeon hole principle to prove that given any five integers, there will be three for which the sum of the squares of those integers is divisible by 3. Ie., suppose your numbers are x_1, x_2, x_3, x_4 and x_5. Then there are three x_i, x_j and x_k such that $x_i^2 + x_j^2 + x_k^2 = 3n$ for some $n \in \mathbb{Z}$. HINT: How many holes do you need to use the Pigeon Hole principle so that three numbers are in one hole?

Lemma: $x^2/3$ only has remainders $[0, 1]$ for $x \in \mathbb{N}$

Possibilities for x, $x = 3k + r, k \in \mathbb{Z}, r \in \{0, 1, 2\}$

$x = 3k$	$x^2 = 9k^2$
$x^2 = 9k^2 = 3(3k^2)$	$x^2 \bmod 3 = 0$
$x = 3k + 1$	$x^2 = 9k^2 + 6k + 1$
$x^2 = 3(3k^2 + 2k) + 1$	$x^2 \bmod 3 = 1$
$x = 3k + 2$	$x^2 = 9k^2 + 12k + 4 = 9k^2 + 12k + 3 + 1$
$x = 3(3k^2 + 4k + 1) + 1$	$x^2 \bmod 3 = 1$

Therefore, $x^2/3$ only has remainders 0 and 1.

$\forall x \in \mathbb{Z}, x^2 = 3k + r, r \in \mathbb{Z}, \in [0, 1]$ **by lemma**.

Let the 5 integers be pigeons, and let the 2 possible remainders be holes.

$5 > 2$ implies that in any scenario, if we choose any 5 integers, there must be atleast 3 with the remainder 0 or atleast 3 with the remainder 1.

Case 1: 3 or more of the numbers squared divided by 3 has the remainder 1. then if we take the sum of the numbers squared, their total remainder is 3, which is divisible by 3.

$$\begin{aligned}
{x_1}^2 + {x_2}^2 + {x_3}^2 &= 3k + 1 + 1 + 1 \\
{x_1}^2 + {x_2}^2 + {x_3}^2 &= 3k + 3 \\
{x_1}^2 + {x_2}^2 + {x_3}^2 &= 3(k + 1) \Rightarrow 3 | x_1^2 + x_2^2 + x_3^2
\end{aligned}$$

Case 2: 3 or more of the numbers squared divided by 3 has the remainder 0. then if we choose the sum those 3 numbers squared, their total remainder is 0, which implies the sum is divisible by 3.

$$\begin{aligned}
{x_1}^2 + {x_2}^2 + {x_3}^2 &= 3k + 0 + 0 + 0 \\
{x_1}^2 + {x_2}^2 + {x_3}^2 &= 3k \Rightarrow 3 | x_1^2 + x_2^2 + x_3^2 = 3k
\end{aligned}$$

Therefore, in all possibility for the 5 x^2 values, atleast 3 of them will be divisible by 3.

6. Consider the following summation:

$$\sum_{i=1}^{n} i2^i = 1 \cdot 2^1 + 2 \cdot 2^2 + 3 \cdot 2^3 + \cdots + n \cdot 2^n$$

Guess a formula for this summation and prove your formula correct using simple induction.

n	$\sum_{i=1}^{n} i2^i =$	result
1	$1 \cdot 2^1$	2
2	$1 \cdot 2^1 + 2 \cdot 2^2$	10
3	$1 \cdot 2^1 + 2 \cdot 2^2 + 3 \cdot 2^3$	34
4	$1 \cdot 2^1 + 2 \cdot 2^2 + 3 \cdot 2^3 + 4 \cdot 2^4$	98
5	$1 \cdot 2^1 + 2 \cdot 2^2 + 3 \cdot 2^3 + 4 \cdot 2^4 + 5 \cdot 2^5$	258
6	$1 \cdot 2^1 + 2 \cdot 2^2 + 3 \cdot 2^3 + 4 \cdot 2^4 + 5 \cdot 2^5 + 6 \cdot 2^6$	642
7	$1 \cdot 2^1 + 2 \cdot 2^2 + 3 \cdot 2^3 + 4 \cdot 2^4 + 5 \cdot 2^5 + 6 \cdot 2^6 + 7 \cdot 2^7$	1538

Tests:

n	$n2^n$	$2^{n-1}(n)$	$2^{n+1}(n)$	$2^{n-1}(n+1)$	$2^{n+1}(n-1)$	$2^{n+1}(n-1)+2$
1	2	1	4	2	0	2
2	8	...	...	6	...	10
3	...	...	...	...	...	34
4	...	...	...	...	...	98

Predicate:

$P(n) = \sum_{i=1}^{n} i2^i = 2^{n+1}(n-1) + 2$

Base case: show n = 1:

$P(n) = \sum_{i=1}^{1} i2^i = 2 \quad 2^{1+1}(1-1) + 2 = 2$

$\therefore$ the case holds for n = 0.

Inductive Hypothesis:

Assume for any arbitrary natural number k, $p > 1, P(k)$ is true.

$P(k) = \sum_{i=1}^{k} i2^i = 2^{k+1}(k-1) + 2$

Inductive step: Prove $P(k) \to P(k+1)$

$$\text{show: } P(k+1) = \sum_{i=1}^{k+1} i2^i = (k+1-1)2^{k+1+1} + 2 = k2^{k+2} + 2$$

$P(k+1) = (k+1)2^{k+1} + \sum_{i=1}^{k} i2^i$

$P(k+1) = (k+1)2^{k+1} + 2^{k+1}(k-1) + 2$ by Inductive Hypothesis

$P(k+1) = k \cdot 2^{k+1} + 2^{k+1} + k \cdot 2^{k+1} - 2^{k+1} + 2$

$P(k+1) = 2^{k+1}2k + 2$

$P(k+1) = 2 = k2^{k+2} + 2$

Since the statement holds for $n = 1$ and $n = k \to k+1$ is also true, $\therefore \sum_{i=1}^{n} i2^i = 2^{n+1}(n-1) + 2$