Discussion 1C Slides

CS 70 Summer 2020

June 26, 2020

Warm-Up

How many integers n divide 12? In other words, how many integers n are there such that $\frac{12}{n}$ is also an integer?

Solution: 12, namely $n = -12, -6, -4, -3, -2, -1, 1, 2, 3, 4, 6, 12$.

Quick Review

Induction and its many flavors

- Basic idea: use the truth of previous things to prove the truth about successive things
- Vanilla Induction: prove $P(0)$ and prove that $P(n) \implies P(n+1)$ for any n.
- Strong Induction: prove $P(0)$ and prove that $(P(0) \wedge P(1) \wedge \cdots \wedge P(n)) \implies P(n+1)$ for any n.
- There are some fancier induction techniques than these two, but all induction techniques make (in some form) the chain below:

$$P(0) \implies P(1) \implies P(2) \implies P(3) \implies P(4) \implies \cdots$$

Divisibility Induction (Dis 1C Problem 1)

Prove that for all $n \in \mathbb{N}$ with $n \geq 1$, the number $n^3 - n$ is divisible by 3. (**Hint**: recall the binomial expansion $(a+b)^3 = a^3 + 3a^2b + 3ab^2 + b^3$)

Solution: Vanilla Induction. We note that $1^3 - 1 = 0$ is divisible by 3, so the base case $n = 1$ holds. Now assume the statement holds for $n = k$ arbitrary. Then observe that for $n = k+1$, we have that

$$(k+1)^3 - (k+1) = (k^3 - k) + 3(k^2 + k),$$

where the first term is divisible by 3 by the inductive hypothesis and the second is always a multiple of 3. Hence the statement holds for $n = k+1$, completing the induction.

Note: A quicker way to prove this is to note that for any n, we have the factorization $n^3 - n = (n-1)(n)(n+1)$ and that no matter what n is, since these terms are three consecutive integers, one of them must be divisible by 3.

Make it Stronger (Disc 1C Problem 2)

Let $x \geq 1$ be a real number. Use induction to prove that for all positive integers n, all of the entries in the matrix

$$\begin{pmatrix} 1 & x \\ 0 & 1 \end{pmatrix}^n$$

are $\leq xn$. (**Hint:** Try writing out the first few powers and see if you can prove something stronger)

Make it Stronger (Disc 1C Problem 2)

Solution: Writing out the first few powers, we see a pattern:

$$\begin{pmatrix} 1 & x \\ 0 & 1 \end{pmatrix}^1 = \begin{pmatrix} 1 & 1x \\ 0 & 1 \end{pmatrix}$$
$$\begin{pmatrix} 1 & x \\ 0 & 1 \end{pmatrix}^2 = \begin{pmatrix} 1 & 2x \\ 0 & 1 \end{pmatrix}$$
$$\begin{pmatrix} 1 & x \\ 0 & 1 \end{pmatrix}^3 = \begin{pmatrix} 1 & 3x \\ 0 & 1 \end{pmatrix}$$

So the key idea here is to strengthen the inductive hypothesis: instead of proving that each entry is $\leq nx$, we can instead prove the stronger statement that

$$\begin{pmatrix} 1 & x \\ 0 & 1 \end{pmatrix}^n = \begin{pmatrix} 1 & nx \\ 0 & 1 \end{pmatrix}.$$

Make it Stronger (Disc 1C Problem 2)

Clearly, this claim holds for $n = 1$, so it remains to prove the inductive step. Assume this claim holds for $n = k$. Then we have that

$$\begin{pmatrix} 1 & x \\ 0 & 1 \end{pmatrix}^{k+1} = \begin{pmatrix} 1 & x \\ 0 & 1 \end{pmatrix} \cdot \begin{pmatrix} 1 & kx \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} 1 & (k+1)x \\ 0 & 1 \end{pmatrix},$$

as desired.

Binary Numbers (Dis 1C Problem 3)

Prove that every positive integer n can be written in binary. In other words, prove that we can write

$$n = c_k \cdot 2^k + c_{k-1} \cdot 2^{k-1} + \cdots + c_1 \cdot 2^1 + c_0 \cdot 2^0,$$

where $k \in \mathbb{N}$ and $c_k \in \{0, 1\}$. (**Hint:** Strong Induction)

Binary Numbers (Dis 1C Problem 3)

Solution: We can write $n = 1 = 1 \cdot 2^0$, so this establishes the base case $n = 1$. Now assume that we can write every integer m with $1 \leq m \leq j$ in binary for j arbitrary. Then we proceed by casework on the parity of $j + 1$. If $j + 1$ is even, then $\frac{j+1}{2}$ is an integer, so since $1 \leq (j + 1)/2 \leq j$, it has a valid binary representation

$$\frac{j+1}{2} = c_k \cdot 2^k + c_{k-1} \cdot 2^{k-1} + \cdots + c_0 \cdot 2^0,$$

so

$$j + 1 = c_k \cdot 2^{k+1} + c_{k-1} \cdot 2^k + \cdots + c_0 \cdot 2^1 + 0 \cdot 2^0,$$

hence $j + 1$ has a valid binary representation.

Binary Numbers (Dis 1C Problem 3)

Now, if $j+1$ is odd, then j is even, so $\frac{j}{2}$ is an integer, and hence since $1 \leq \frac{j}{2} \leq j$, it has a valid binary representation

$$\frac{j}{2} = c_k \cdot 2^k + c_{k-1} \cdot 2^{k-1} + \cdots + c_0 \cdot 2^0,$$

so it follows that

$$j+1 = c_k \cdot 2^{k+1} + c_{k-1} \cdot 2^k + \cdots + c_0 \cdot 2^1 + 1 \cdot 2^0,$$

which is again a valid binary representation of $j+1$. These cases are exhaustive, so we have proved the claim.

Division Algorithm (Dis 1C Problem 4)

Let $a, b \in \mathbb{Z}$, $b \neq 0$. In this problem, we will prove, using the WOP, that there exists unique integers q, r such that $0 \leq r < |b|$ and $a = qb + r$. Here, q is called the *quotient* and r is called the *remainder*.

(a) Let $A = \{a - qb | q \in \mathbb{Z} \wedge a - qb \geq 0\}$. Show that A is non-empty (keep in mind that we must consider the case where a is negative).

(b) Use the WOP to show that there exists $q, r \in \mathbb{Z}$ such that $a = qb + r$, and $0 \leq r < |b|$.

(c) Show that the q and r from part b are unique.

Division Algorithm (Dis 1C Problem 4)

(a) Let $A = \{a - qb | q \in \mathbb{Z} \wedge a - qb \geq 0\}$. Show that A is non-empty (keep in mind that we must consider the case where a is negative).

Solution: If $a \geq 0$, then we can let $q = 0$. Then $a - qb = a \geq 0$, so A has an element. If $a < 0$, then we can let $q = ab$. Then $a - qb = a(1 - b^2)$. Since b is a nonzero integer, $b^2 \geq 1$, so $1 - b^2 \leq 0$, thus since $a < 0$, the product $a(1 - b^2)$ is nonnegative, hence A has an element in this case as well. This is exhaustive, so we're done.

Division Algorithm (Dis 1C Problem 4)

(b) Use the WOP to show that there exists $q, r \in \mathbb{Z}$ such that $a = qb + r$, and $0 \leq r < |b|$.

Solution: Since A is a nonempty set of nonnegative integers, it has a smallest element, hence there exists a q such that $a - qb$ is minimal. Now if $r = a - qb \geq |b|$, then one of $q' = q - 1$ or $q' = q + 1$ (depending on the sign of b) will generate $a - q'b = r - |b| \geq 0$, which contradicts the minimality of r. Thus, $0 \leq r < |b|$, as desired.

Division Algorithm (Dis 1C Problem 4)

(c) Show that the q and r from part b are unique.

Solution: Suppose that there were two pairs q, r and q', r' such that $a = qb + r = q'b + r'$. Then we have that $(q - q')b = r' - r$. This means that $q - q' = 0$ or $r' - r$ is divisible by b. In the first case, this means that $q' = q$ so $r = r'$, and in the second, it means that $r' = r$, so again $q' = q$. Thus, they must be the same pair, and therefore q, r are unique.