1 Week 2: February 6 - 13, 2019

1.1 Mathematical Induction

Theorem 1.1 (Mathematical Induction). [1]

Let $n_0 \in \mathbb{N} \cup \{0\}$ and let $P(n)$ be a statement for each natural number $n \geq n_0$. If

1. *The statement $P(n_0)$ is true.*
2. *For all $k \geq n_0$, the truth of $P(k)$ implies the truth of $P(k+1)$.*

then $P(n)$ is true for all $n \in \mathbb{N}$.

Note in class we assumed for the inductive step that $P(n)$ is true for all $n \leq k$ such that $n, k \in \mathbb{N}$.

Example 1.1. Prove using induction

$$\sum_{i=0}^{n} 2^i = 2^{n+1} - 1$$

First, check the base case $n = 0$

$$\sum_{i=0}^{0} 2^0 = 2^{0+1} - 1 \checkmark$$

by the inductive hypothesis assume for all $k \geq 0$ is true, namely,

$$\sum_{i=0}^{k} 2^i = 2^{k+1} - 1$$

Now show $P(k+1)$

$$\sum_{i=0}^{k+1} 2^i = 2^{(k+1)+1} - 1$$

is true. Return to the inductive hypothesis and show it implies $P(k+1)$ by adding 2^{k+1} to both sides

$$\sum_{i=0}^{k} 2^i + 2^{k+1} = 2^{k+1} - 1 + 2^{k+1}$$

$$\sum_{i=0}^{k+1} 2^i = 2 \cdot 2^{k+1} - 1 = 2^{k+2} - 1 = 2^{(k+1)+1} - 1$$

[1] Bartle, R., Sherbert, D. (2000). *Introduction to Real Analysis.* New York, NY: Wiley & Sons. p. 13

2 Other Number Worlds

There are other sets of numbers, and some of the those sets do not have unique prime factorizations. For example, the set of numbers $\mathbb{Z}$ adjoin $\sqrt{-5}$ do not have unique factorizations. Numbers in the set of $\mathbb{Z}$ adjoin $\sqrt{-5}$ have the form

$$a + b\sqrt{-5}, \quad a, b \in \mathbb{Z}$$

the product of two numbers in $\mathbb{Z}$ adjoin $\sqrt{-5}$ is defined by

$$(a + b\sqrt{-5})(c + d\sqrt{-5}) = ac + ad\sqrt{-5} + cb\sqrt{-5} - 5bd = (ac - 5bd) + (ad + cb)\sqrt{-5}$$

From this definition it is possible to show that $6 = 6 + 0\sqrt{-5}$ does not have a unique prime factorization, namely,

$$6 = (2 - 0\sqrt{-5})(3 + 0\sqrt{-5}) \quad \text{or} \quad 6 = (1 - \sqrt{-5})(1 + \sqrt{-5})$$

From the above observation we ask the question or questions, "Do the integers, $\mathbb{Z}$, have a unique factorization?" or "why do the integers, $\mathbb{Z}$, have a unique factorization?"

2.1 Euclid's Division Lemma

Theorem 2.1 (Euclid's Division Lemma)**.** *For all $j, k \in \mathbb{N}$ there exists unique $q, r \in \mathbf{N}$ such that*

$$0 \leq r < k \quad \textit{and} \quad j = qk + r$$

Proof. Break the proof into two parts: one for existence and one for uniqueness. Start first with existence by constructing q and r. Construct q from j and k as

$$q = \left\lfloor \frac{j}{k} \right\rfloor$$

Where $\lfloor \ \rfloor$ is a well defined function that rounds rational numbers down to the nearest natural number. This establishes the existence of q. Now we can use it and j and k to construct r, namely,

$$r = j - qk$$

Now work to establish $0 \leq r < k$. By definition

$$\left\lfloor \frac{j}{k} \right\rfloor \leq \frac{j}{k} \implies \frac{j}{k} - 1 < \left\lfloor \frac{j}{k} \right\rfloor \leq \frac{j}{k}$$

multiply through by k

$$j - k < \left\lfloor \frac{j}{k} \right\rfloor k \leq j \implies qk + r - k < qk \leq qk + r$$

subtract through the inequality by qk

$$r - k < 0 \leq r$$

Now take each inequality in turn, namely,

$$r - k < 0 \implies r < k \qquad \text{and} \qquad 0 \leq r$$

This completes the existence part of the proof. In order to prove uniqueness argue by contradiction. Suppose for all $j, k \in \mathbb{N}$ there exists q' and r' that also satisfy $j = q'k + r'$ and $0 \leq r' < k$.

$$q'k + r' = qk + r \implies r' - r = qk - q'k \implies r' - r = k(q - q')$$

since $0 \leq r < k$ and $0 \leq r' < k$

$$|\, r - r' \,| < k \implies k > |\, r - r' \,| = |\, k(q - q') \,|$$

this is a contradiction if $q \neq q'$. So if $q - q' = 0$ then $r - r' = 0$ or $q = q'$ and $r = r'$ or q and r are unique.

□

2.2 Greatest Common Divisor

Definition 2.1. If a, b and $q \in \mathbb{Z}$, then a *divides* b, denoted $a|b$ such that $b = qa$. Also, a is called a divisor of b.

Definition 2.2. If $a, b \in \mathbb{Z}$ and not both are zero, then $d \in \mathbb{Z}$ is called a *common divisor* of a and b, if

(i) $d > 0$

(ii) $d \mid a$ and $d \mid b$

(iii) If $f \mid a$ and $f \mid b$ then $f \mid d$.

Example 2.1. If $2 \mid 6$ then by definition $6 = 2(3)$

Example 2.2.

$$3 \not| \, 5$$

Example 2.3.

$$a|0 \implies 0 = aq \implies 0 = a(0)$$

Theorem 2.2. *If $a, b \in \mathbb{N}$, then the gcd(a, b) exists and is unique.*

Proof. Use the Euclidean Division Algorithm

$$a = bq_1 + r_1, \quad 0 \leq r_1 < b$$

If $r_1 > 0$ there exist q_2 and r_2 such that

$$b = r_1 q_2 + r_2, \quad 0 \leq r_2 < r_1$$

If $r_2 > 0$, then there exist q_3 and r_3 such that

$$r_1 = r_2 q_3 + r_3, \quad 0 \leq r_3 < r_2$$

If $r_3 > 0$, then there exist q_4 and r_4 such that

$$r_2 = r_3 q_4 + r_4, \qquad 0 \leq r_4 < r_3$$

repeat the algorithm until $r_n = 0$ so that the last application of the algorithm yields

$$r_{n-2} = r_{n-1} q_n + r_n, \quad \text{and} \quad r_n = 0$$

Now use induction to prove $r_{n-1} \mid b$ and ultimately a. The base case is when $r_n = 0$, so

$$r_{n-2} = r_{n-1} q_n \implies r_{n-1} \mid r_{n-2} \quad \checkmark$$

Now by the inductive hypothesis assume $r_{k-2} = r_{k-1} q_k + r_k$ is true and assume $r_{n-1} \mid r_{k-2}$ and $r_n \mid r_{k-1}$. By definition of divisibility, $r_{k-2} = u r_{n-1}$ and $r_{k-1} = v r_{n-1}$. Substituting into inductive hypothesis

$$u r_{n-1} = v r_{n-1} q_k + r_k \implies r_k = (u - v q_k) r_{n-1} \implies r_{n-1} \mid r_k$$

so by induction $r_{n-1} \mid b$.

Now assume $f \in \mathbb{Z}$ and $f \mid a$ and $f \mid b$. By condition (iii) in the definition of common divisor $f \mid d$. Use induction to show that f divides $r_2, \ldots, r_{n-1}$. In order to prove the base case note that if $f \mid a$ and $f \mid b$ then

$$\begin{matrix} a = b q_1 + r_1 \\ b = r_1 q_2 + r_2 \end{matrix} \implies \begin{matrix} kf = lf q_1 + r_r \\ lf = r_1 q_2 + r_2 \end{matrix} \implies lf = (kf - lf q_1) q_2 + r_2$$

$$\implies r_2 = f(f - k q_2 + l q_1 q_2) \implies f \mid r_2 \checkmark$$

By the inductive hypothesis assume $f \mid r_2, f \mid r_3, \ldots, f \mid k$ and

$$r_{k-2} = r_{k-1} q_k + r_k$$

is true. So by the inductive hypothesis $r_{k-2} = rf$, $r_{k-1} = sf$ and $r_k = tf$, therefore substituting

$$tf = (rf - sf q_k) q_{k+1} + r_{k+1} \implies r_{k+1} = f(t - r q_{k+1} + s q_k q_{k+1}) \implies f \mid r_{k+1}$$

and this completes the existence part of the proof. Now in order to establish uniqueness assume there exist $d_1, d_2 \in \mathbb{Z}$ that are both greatest common divisors of $a, b \in \mathbb{Z}$. By definition of common divisor if $d_1 \mid a$ and $d_1 \mid b$, then $d_1 \mid d_2$; likewise, if $d_2 \mid a$ and $d_2 \mid b$, then $d_2 \mid d_1$ which implies

$$d_2 = k d_1 \qquad \text{and} \qquad d_1 = j d_2 \implies d_1 = j(k d_1)$$

Since $d_1, d_2, j, k \in \mathbb{Z}$ then $j = k = 1$ and $d_1 = d_2$ which proves uniqueness.

$\square$

Example 2.4. Find the $\gcd(391, 272)$

$$391 = 272(1) + 119 \implies 272 = 119(2) + 34 \implies 119 = 34(3) + 17 \implies 34 = 17(2)$$

$$\gcd(391, 272) = 17$$

Question for next class: Let $F_0 = 1, \quad F_1 = 1$ and $F_n = F_{n-1} + F_{n-2}$

1. What is the $\gcd(F_n, F_{n-1})$ for some fixed n.
2. How many steps does it take using Euclid's Algorithm in terms of n.