Divide & Conquer Proofs

Karim El Shenawy

December 2020

Introduction

This course notebook is the collection of theorem proofs, exercises and answers from Unit 1 of the Number Theory Through Inquiry (Mathematical Association of America Textbooks).

Divisibility & Congruence

1.1 Theorem

Let a, b, and c be integers. If $a|b$ and $a|c$, then $a|(b+c)$.

Proof. Our hypothesises that $a|b$ and $a|c$ both mean respectively, by definition, that $b = k_1a$ and $c = k_2a$ for some integer k_1 and k_2. Also by definition, $a|(b+c)$ means that $b+c = k_3a$ for some integer k_3. Using that we can say that $b+c = k_1a+k_2a = a(k_1+k_2) = k_3a$. Thus by definition, $a|a(k_1+k_2)$, knowing that $(b+c) = a(k_1+k_2)$, we can satisfy the definition of $a|(b+c)$. □

1.2 Theorem

Let a, b, and c be integers. If $a|b$ and $a|c$, then $a|(b-c)$.

Proof. Our hypothesises that $a|b$ and $a|c$ both mean respectively, by definition, that $b = k_1a$ and $c = k_2a$ for some integer k_1 and k_2. Also by definition, $a|(b-c)$ means that $b-c = k_3a$ for some integer k_3. Using that we can say that $b-c = k_1a-k_2a = a(k_1-k_2) = k_3a$. Thus by definition, $a|a(k_1-k_2)$, knowing that $(b-c) = a(k_1-k_2)$, we can satisfy the definition of $a|(b-c)$. □

1.3 Theorem

Let a, b, and c be integers. If $a|b$ and $a|c$, then $a|bc$.

Proof. Our hypothesises that $a|b$ and $a|c$ both mean respectively, by definition, that $b = k_1a$ and $c = k_2a$ for some integer k_1 and k_2. Also by definition, $a|bc$ means that $bc = (k_1a)(k_2a) = k_1k_2a^2$. Using that we can say that $bc =$

$k_1k_2a^2 = (k_1k_2a)a$. Thus by definition, $a|(k_1k_2a)$, knowing that $bc = (k_1k_2a)a$, we can satisfy the definition of $a|bc$. □

1.4 Question

Can you weaken the hypothesis of the previous theorem and still prove the conclusion? Can you keep the same hypothesis, but replace the conclusion by the stronger conclusion that $a^2|bc$ and still prove the theorem?

We can say that

1.5 Question

Can you formulate your own conjecture along the lines of the above theorems and then prove it to make your theorem?

1.6 Theorem

Let a, b, and c be integers. If $a|b$, then $a|bc$.

Proof. Based off of Theorem 1.4, we can deduce that □

1.7 Exercise

1. *Is* $45 \equiv 9 \pmod 4$*?*
   Yes, since $4|(45 - 9) = 4|36$ and 4 does divide 36.

2. *Is* $37 \equiv 2 \pmod 5$*?*
   Yes, since $5|(37 - 2) = 5|35$ and 5 does divide 35.

3. *Is* $37 \equiv 3 \pmod 5$*?*
   No, since $5|(37 - 3) = 5|34$ and 5 does not divide 34.

4. *Is* $37 \equiv -3 \pmod 5$*?*
   Yes, since $5|(37 - (-3)) = 5|40$ and 5 does divide 40.

1.8 Exercise

1. $m \equiv 0 \pmod 3$.
   m can be any integer such that $3|m$ thus m can be any integer from $\{-3(N), -3(N-1)...-3(1), 3(1), 3(2), 3(3), 12, 15...3(N-1), 3(N)\}$ where is N is the length of the set.

2. $m \equiv 1 \pmod 3$.
   m can be any integer such that $3|(m + 1)$ thus m can be any integer from $\{-3(N) - 1, -3(N - 1) - 1... - 3(1) - 1, 3(1) - 1, 3(2) - 1, 3(3) - 1, 11, 14...3(N - 1) - 1, 3(N) - 1\}$ where is N is the length of the set.

3. $m \equiv 2 \pmod 3$.
   m can be any integer such that $3|(m+2)$ thus m can be any integer from $\{-3(N)-2, -3(N-1)-2 ... -3(1)-2, 3(1)-2, 3(2)-2, 3(3)-2, 10, 13 ... 3(N-1)-2, 3(N)-2\}$ where is N is the length of the set.

4. $m \equiv 3 \pmod 3$.
   m can be any integer such that $3|m$ thus m can be any integer from $\{-3(N), -3(N-1) ... -3(1), 3(1), 3(2), 3(3), 12, 15 ... 3(N-1), 3(N)\}$ where is N is the length of the set.

5. $m \equiv 4 \pmod 3$.
   m can be any integer such that $3|m+4$ thus m can be any integer from $\{-3(N)-1, -3(N-1)-1 ... -3(1)-1, 3(1)-1, 3(2)-1, 3(3)-1, 11, 14 ... 3(N-1)-1, 3(N)-1\}$ where is N is the length of the set.

1.9 Theorem

Let a, and n be integers with $n > 0$. Then $a \equiv a \pmod n$.

Proof. □

1.10 Theorem

Let a, b, and n be integers with $n > 0$.Then$a \equiv a \pmod n$.

Proof. □