Divide & Conquer Proofs

Karim El Shenawy

January 2021

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 $bc =$

$k_1 k_2 a^2 = (k_1 k_2 a)a$. Thus by definition, $a|(k_1 k_2 a)$, knowing that $bc = (k_1 k_2 a)a$, 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 weaken the hypothesis by saying that by definition, if $a|c$ is true then $a\ vertkc$ for some integer k. We can then maintain the same hypothesis and also state that because $bc = (k_1 a)(k_2 a) = k_1 k_2 a^2$, $a^2|bc$

1.5 Question

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

We can formulate the following conjecture: *Let a, b and c be integers. If $a|b$ and $a|c$ then $a|t$ where t is the sum, difference or the multiplication total of b and c.*

Proof. Using theorems 1.1, 1.2 and 1.3, we can proof this 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. By Definition, the statement above can be written as $n|a-a$ which would also mean that $n|0$. And n does divide 0 with the following logic $0 = n * 0$. □

1.10 Theorem

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

Proof. By definition, we can represent the above statements as $n|a-b$ and $n|b-a$. Using the Theorem 1.2 proved above we can deduce that this is true. □

1.11 Theorem

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

Proof. By definition, $a \equiv b \pmod n$ can be represented as:

$$(a-b) = nk \qquad \text{for a given integer k}$$

$$\Rightarrow \qquad 1) b = a - nk$$

Similarly,

$$(c-b) = ns \qquad \text{for a given integer s}$$

$$\Rightarrow \qquad 2) b = c - ns$$

Now equating 1) and 2),

$$
\begin{aligned}
& c = c \\
\Rightarrow \quad & a - nk = c - ns \\
\Rightarrow \quad & a - c = nk - ns \\
\Rightarrow \quad & a - c = n(k - s)
\end{aligned}
$$

Thus, satisfying the claim that $a \equiv c \pmod{n}$. □

1.12 Theorem

Let a, b, c, d and n be integers with $n > 0$. If $a \equiv b \pmod{n}$ and $c \equiv d \pmod{n}$ then $a + c \equiv b + d \pmod{n}$

Proof. By definition, $a \equiv b \pmod{n}$ can be represented as:

$$
\begin{aligned}
& (a - b) = nk && \text{for a given integer k} \\
\Rightarrow \quad & 1) b = a - nk
\end{aligned}
$$

Similarly,

$$
\begin{aligned}
& (c - d) = ns && \text{for a given integer s} \\
\Rightarrow \quad & 2) d = c - ns
\end{aligned}
$$

Now adding 1) and 2),

$$
\begin{aligned}
& b + d = (a - nk) + (c - ns) \\
\Rightarrow \quad & b + d = a + c - n(k + s) \\
\Rightarrow \quad & n(k + s) = (a + c) - (b + d)
\end{aligned}
$$

Thus, satisfying the claim that $a + c \equiv b + d \pmod{n}$. □

1.13 Theorem

Let a, b, c, d and n be integers with $n > 0$. If $a \equiv b \pmod{n}$ and $c \equiv d \pmod{n}$ then $a - c \equiv b - d \pmod{n}$

Proof. By definition, $a \equiv b \pmod{n}$ can be represented as:

$$
\begin{aligned}
& (a - b) = nk && \text{for a given integer k} \\
\Rightarrow \quad & 1) b = a - nk
\end{aligned}
$$

Similarly,

$$
\begin{aligned}
& (c - d) = ns && \text{for a given integer s} \\
\Rightarrow \quad & 2) d = c - ns
\end{aligned}
$$

Now subtracting 1) and 2),

$$
\begin{aligned}
& b-d = (a-nk)-(c-ns) \\
\Rightarrow \quad & b-d = a-c-n(k+s) \\
\Rightarrow \quad & n(k+s) = (a-c)-(b-d)
\end{aligned}
$$

Thus, satisfying the claim that $a - c \equiv b - d \pmod{n}$. □

1.14 Theorem

Let a, b, c, d and n be integers with $n > 0$. If $a \equiv b \pmod{n}$ and $c \equiv d \pmod{n}$ then $ac \equiv bd \pmod{n}$

Proof. By definition, $a \equiv b \pmod{n}$ can be represented as:

$$
\begin{aligned}
& (a-b) = nk && \text{for a given integer k} \\
\Rightarrow \quad & 1)b = a-nk
\end{aligned}
$$

Similarly,

$$
\begin{aligned}
& (c-d) = ns && \text{for a given integer s} \\
\Rightarrow \quad & 2)d = c-ns
\end{aligned}
$$

Now multiplying 1) and 2),

$$
\begin{aligned}
& bd = (a-nk)(c-ns) \\
\Rightarrow \quad & bd = ac - a(ns) - c(nk) + (nk)(ns) \\
\Rightarrow \quad & bd = ac - n*(a(s) - c(k) + n(k)(s))
\end{aligned}
$$

Thus, satisfying the claim that $ac \equiv bd \pmod{n}$. □

1.15 Theorem

Let a, b and n be integers with $n > 0$. Show that if $a \equiv b \pmod{n}$ then $a^2 \equiv b^2 \pmod{n}$

Proof. $a^2 \equiv b^2 \pmod{n}$ can be represented as $a(a) \equiv b(b) \pmod{n}$ by exponential property. Based off Theorem 1.14, we know that $ac \equiv bd \pmod{n}$ if $a \equiv b \pmod{n}$ and $c \equiv d \pmod{n}$. This shows that $a^2 \equiv b^2 \pmod{n}$ is true. □

1.16 Theorem

Let a, b and n be integers with $n > 0$. Show that if $a \equiv b \pmod{n}$ then $a^3 \equiv b^3 \pmod{n}$

Proof. By properties of exponents, $a^3 \equiv b^3 \pmod{n}$ can be represented as $(a)a^2 \equiv (a)b^2 \pmod{n}$. Using theorems 1.14 and 1.15, we can satisfy that $a^3 \equiv b^3 \pmod{n}$ is true. □

1.17 Theorem

Let a, b, k and n be integers with $n > 0$ and $k > 1$. Show that if $a \equiv b \pmod{n}$ and $a^{k-1} \equiv b^{k-1} \pmod{n}$, then

$$a^k \equiv b^k \pmod{n}$$

Proof. By properties of exponents, we can present the above statement as

$$\begin{aligned} a^k &\equiv b^k \pmod{n} \\ a^k a^1 a^{-1} &\equiv b^k b^1 b^{-1} \pmod{n} \\ a^1 a^{k-1} &\equiv b^1 b^{k-1} \pmod{n} \end{aligned}$$

Knowing that $a \equiv b \pmod{n}$ and $a^{k-1} \equiv b^{k-1} \pmod{n}$ and theorem 1.14, we can satisfy that $a^k \equiv b^k \pmod{n}$. □

1.18 Theorem

Let a, b, k and n be integers with $n > 0$ and $k > 1$. Show that if $a \equiv b \pmod{n}$, then

Proof. **Base case (k = 1):**

$$\begin{aligned} a^k &\equiv b^k \pmod{n} \\ a^1 &\equiv b^1 \pmod{n} \end{aligned}$$

Thus making the statement true if k = 1.
Inductive Hypothesis: Assume k = h + 1
Inductive Step:

$$\begin{aligned} a^k &\equiv b^k \pmod{n} \\ a^{h+1} &\equiv b^{h+1} \pmod{n} \\ a^h a &\equiv b^h b \pmod{n} && \text{(Exponential Property)} \end{aligned}$$

By theorem 1.14, we know that $a \equiv b \pmod{n}$ and $c \equiv d \pmod{n}$ then $ac \equiv bd \pmod{n}$. This helps satisfies $a^{h+1} \equiv b^{h+1} \pmod{n}$ since $a^h \equiv b^h \pmod{n}$ and $a \equiv b \pmod{n}$. □

1.19 Theorem

- **1.12 Theorem**
- **1.13 Theorem**
- **1.14 Theorem**
- **1.15 Theorem**

- **1.16 Theorem**
- **1.17 Theorem**
- **1.18 Theorem**

1.20 Theorem

Let a, b, c and n be integers for which $ac \equiv bc \pmod{n}$. Can we conclude that $a \equiv b \pmod{n}$?

Proof. □

1.21 Theorem

Let ?

Proof. □

1.22 Theorem

Let ?

Proof. □

1.23 Theorem

Let ?

Proof. □

1.24 Exercise

Let ?

Proof. □

1.25 Exercise

Let ?

Proof. □

1.26 Exercise

Let ?

Proof. □

1.27 Exercise

Let ?

Proof. □

1.28 Exercise

Let ?

Proof. □

1.29 Exercise

Let ?

Proof. □

1.30 Exercise

Let ?

Proof. □

1.31 Exercise

Let ?

Proof. □

1.32 Exercise

Let ?

Proof. □

1.33 Exercise

Let ?

Proof. □

1.34 Exercise

Let ?

Proof. □

1.35 Exercise

Let ?

Proof. ☐

1.36 Exercise

Let ?

Proof. ☐

1.37 Exercise

Let ?

Proof. ☐

1.38 Exercise

Let ?

Proof. ☐

1.39 Exercise

Let ?

Proof. ☐

1.40 Exercise

Let ?

Proof. ☐

1.41 Exercise

Let ?

Proof. ☐

1.42 Exercise

Let ?

Proof. ☐

1.43 Exercise

Let ?

Proof. $\square$

1.44 Exercise

Let ?

Proof. $\square$

1.45 Exercise

Let ?

Proof. $\square$

1.46 Exercise

Let ?

Proof. $\square$

1.47 Exercise

Let ?

Proof. $\square$

1.48 Exercise

Let ?

Proof. $\square$

1.49 Exercise

Let ?

Proof. $\square$

1.50 Exercise

Let ?

Proof. $\square$

1.51 Exercise

Let ?

Proof. $\square$

1.52 Exercise

Let ?

Proof. $\square$

1.53 Exercise

Let ?

Proof. $\square$

1.54 Exercise

Let ?

Proof. $\square$

1.55 Exercise

Let ?

Proof. $\square$

1.56 Exercise

Let ?

Proof. $\square$

1.57 Exercise

Let ?

Proof. $\square$

1.58 Corollary

Let ?

Proof. $\square$

1.59 Exercise

Let ?

Proof. $\square$