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 $bc =$

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

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 $a|kc$ for some integer k. We can then maintain the same hypothesis and also state that because $bc = (k_1a)(k_2a) = k_1k_2a^2$, $a^2|bc$

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. $\square$

1.6 Theorem

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

Proof. By definition, we can deduce that $bc = ka$ where $k \in \mathbb{Z}$ since $a|b$ then $b = na$ where $n \in \mathbb{Z}$. Substituting b,

$$\begin{aligned} bc &= ka \\ (na)c &= ka \\ a(nc) &= a(k) \\ (nc) &= (k) \end{aligned}$$

Which ca n be expressed as $c|k$. Therefore, we can conclude that $bc = ka$ is true.

$\square$

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 $0 = n * 0$. $\square$

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. $\square$

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),

$$c = c$$
$$\Rightarrow \qquad a - nk = c - ns$$
$$\Rightarrow \qquad a - c = nk - ns$$
$$\Rightarrow \qquad a - c = n(k-s)$$

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

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:

$$(a-b) = nk \qquad \text{for a given integer k}$$
$$\Rightarrow \qquad 1)b = a - nk$$

Similarly,

$$(c-d) = ns \qquad \text{for a given integer s}$$
$$\Rightarrow \qquad 2)d = c - ns$$

Now adding 1) and 2),

$$b + d = (a - nk) + (c - ns)$$
$$\Rightarrow \qquad b + d = a + c - n(k+s)$$
$$\Rightarrow \qquad n(k+s) = (a+c) - (b+d)$$

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

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:

$$(a - b) = nk \qquad \text{for a given integer k}$$
$$\Rightarrow \quad 1) b = a - nk$$

Similarly,

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

Now subtracting 1) and 2),

$$b - d = (a - nk) - (c - ns)$$
$$\Rightarrow \quad b - d = a - c - n(k + s)$$
$$\Rightarrow \quad n(k + s) = (a - c) - (b - d)$$

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:

$$(a - b) = nk \qquad \text{for a given integer k}$$
$$\Rightarrow \quad 1) b = a - nk$$

Similarly,

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

Now multiplying 1) and 2),

$$bd = (a - nk)(c - ns)$$
$$\Rightarrow \quad bd = ac - a(ns) - c(nk) + (nk)(ns)$$
$$\Rightarrow \quad bd = ac - n * (a(s) - c(k) + n(k)(s))$$

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

$$a^k \equiv b^k \pmod{n}$$
$$a^k a^1 a^{-1} \equiv b^k b^1 b^{-1} \pmod{n}$$
$$a^1 a^{k-1} \equiv b^1 b^{k-1} \pmod{n}$$

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):**

$$a^k \equiv b^k \pmod{n}$$
$$a^1 \equiv b^1 \pmod{n}$$

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** $n = 3, a = 2, b = 17, c = 1$ and $d = 19$ then $2 + 1 \equiv 17 + 19 \pmod{3}$
- **1.13 Theorem** $n = 3, a = 2, b = 17, c = 1$ and $d = 19$ then $2 - 1 \equiv 17 - 19 \pmod{3}$
- **1.14 Theorem** $n = 3, a = 2, b = 17, c = 1$ and $d = 19$ then $2 * 1 \equiv 17 * 19 \pmod{3}$
- **1.15 Theorem** $n = 3, a = 2, b = 17$ then $2^2 \equiv 17^2 \pmod{3}$
- **1.16 Theorem** $n = 3, a = 2, b = 17$ then $2^3 \equiv 17^3 \pmod{3}$
- **1.17 Theorem** $n = 3, a = 2, b = 17$ then $2^k \equiv 17^k \pmod{3}$ where $k \in \mathbb{Z}$ and $k > 1$
- **1.18 Theorem** $n = 3, a = 2, b = 17$ then $2^k \equiv 17^k \pmod{3}$ where $k \in \mathbb{Z}$ and $k > 1$

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. By counterexample, given $a = 1, b = 17, c = 2$ and $n = 3$ where $ac \equiv bc \pmod{n}$ with $1(2) \equiv 17(2) \pmod{3}$. However, we can not conclude that $1 \equiv 17 \pmod{3}$. □

1.21 Theorem

Let a natural number n be expressed in base 10 as

$$n = a_k a_{k-1} ... a_1 a_0$$

If $m = a_k + a_{k+1} + ... + a_1 + a_0$*, then* $n \equiv m \pmod 3$.

Proof. By definition, $n \equiv m \pmod 3$ can be expressed as:

$$3|n - m$$

□

By theorem 1.2, for this theorem to be true, $3|n$ and $3|m$ must be true.

1.22 Theorem

If a natural number is divisible by 3, then when expressed in base 10 , the sum of its digits is divisible by 3.

Proof. Suppose natural number $n = a_k a_{k-1} ... a_1 a_0$ and sum of its digits $m = a_k + a_{k+1} + ... + a_1 + a_0$. We can use theorem 1.21 to prove this. □

1.23 Theorem

If the sum of the digits of a natural number expressed in base 10 is divisible by 3, then the number is divisible by 3 as well.

Proof. Suppose natural number $n = a_k a_{k-1} ... a_1 a_0$ and sum of its digits $m = a_k + a_{k+1} + ... + a_1 + a_0$. We can use theorem 1.21 to prove this. □

1.24 Exercise

Suppose natural number $n = a_k a_{k-1} ... a_1 a_0$ *and sum of its digits* $m = a_k + a_{k+1} + ... + a_1 + a_0$*. If the sum is divisible by 6, then the natural number is 3.*

Proof. By theorem 1.21, since 6 is divisible by 3 as well. □

1.25 Exercise

1. $m = 25, n = 7$

$$\begin{aligned} m &= nq + r \\ 25 &= 7q + r \\ 25 &= 7 \times 3 + 4 \\ 3 &= 7 \times 1 + 3 \\ 7 &= 4 \times 1 + 3 \end{aligned}$$

$$q = 3, r = 4$$

2. $m = 277, n = 4$

$$\begin{aligned} m &= nq + r \\ 277 &= 4q + r \\ 277 &= 4 \times 69 + 1 \\ 4 &= 4 \times 1 + 0 \end{aligned}$$

$q = 69, r = 1$

3. $m = 33, n = 11$

$$\begin{aligned} m &= nq + r \\ 33 &= 11q + r \\ 33 &= 11 \times 3 + 0 \end{aligned}$$

$q = 3, r = 0$

4. $m = 33, n = 45$

$$\begin{aligned} m &= nq + r \\ 33 &= 45q + r \\ 33 &= 45 \times 0 + 33 \end{aligned}$$

$q = 1, r = -12$

1.26 Theorem

Prove the existence part of the Division Algorithm. (Hint: Given n and m, how will you define q? Once you choose this q, then how is r chosen? Then show that $0 \leq r \leq n - 1$.)

Proof. □

1.27 Theorem

Prove the uniqueness part of the Division Algorithm. (Hint: If $nq + r = nq^{'} + r^{'}$, then $nq - nq^{'} = r^{'} - r$. Use what you know about r and $r^{'}$ as part of your argument that $q = q^{'}$.

Proof. □

1.28 Theorem

Let a, b and n be integers with n ¿ 0. Then $a \equiv b \pmod{n}$ if and only if a and b have the same remainder when divided by n. Equivalently, $a \equiv b \pmod{n}$ if and only if when $a = nq_1 + r_1$ $(0 \leq r_1 \leq n-1)$ and $b = nq_2 + r_2$ $(0 \leq r_2 \leq n-1)$, then $r_1 = r_2$.

Proof. □

1.29 Question

Do every two integers have a least one common divisor?

Proof. □

1.30 Question

Can two integers have infinitely many common divisors?

Proof. □

1.31 Exercise

Find the the following greatest common divisors. Which pairs are relatively prime?

1. (36, 22)
2. (45, -15)
3. (-296, -88)
4. (0, 256)
5. (15, 28)
6. (1, -2436)

1.32 Theorem

Let a, n, b, r and k be integers. If $a = nb + r$ and $k|a$ and $k|b$, then $k|r$.

Proof. □

1.33 Theorem

Let a, b, n_1, and r_1 be integers with a and b not both 0. If $a = n_1 b + r_1$, then $(a, b) = (b, r_1)$.

Proof. □

1.34 Exercise

Use the above theorem (Euclidean Algorithm) to show that if $a = 51$ and $b = 15$, then $(51, 15) = (6, 3) = 3$.

Proof. □

1.35 Exercise (Euclidean Algorithm)

Devise a procedure for finding the greatest common divisor of two integers using the previous theorem and the Division Algorithm.

Proof. □

1.36 Exercise

Use the Euclidean Algorithm to find

1. (96, 112)
2. (162, 31)
3. (0, 256)
4. (-288, -166)
5. (1, -2436)

1.37 Exercise

Find integers x and y such that $162x + 31y = 1$.

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. ∎

1.44 Exercise

Let ?

Proof. ∎

1.45 Exercise

Let ?

Proof. ∎

1.46 Exercise

Let ?

Proof. ∎

1.47 Exercise

Let ?

Proof. ∎

1.48 Exercise

Let ?

Proof. ∎

1.49 Exercise

Let ?

Proof. ∎

1.50 Exercise

Let ?

Proof. □

1.51 Exercise

Let ?

Proof. □

1.52 Exercise

Let ?

Proof. □

1.53 Exercise

Let ?

Proof. □

1.54 Exercise

Let ?

Proof. □

1.55 Exercise

Let ?

Proof. □

1.56 Exercise

Let ?

Proof. □

1.57 Exercise

Let ?

Proof. □

1.58 Corollary

Let ?

Proof. $\square$

1.59 Exercise

Let ?

Proof. $\square$