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 $a|bc$. □

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. □

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.

□

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:

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

Similarly,

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

Now equating 1) and 2),

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

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:

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

Similarly,

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

Now adding 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 $a + c \equiv b + d \pmod{n}$. □

1.13 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

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

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:

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

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. Suppose m and n both integers and positive where $m > n$. Given the equation $m - nq$, where $q \in \mathbb{Z}$, results to a set of non-negative integers S. Since $m > n$, S is non empty.
The set S represents the remainders and let r be the smallest element with $0 \leq r$.
By contradiction, since $r = m - nq$, if $r \geq n$, then $m - n(q) - n = r - n \iff m - n(q + 1) = r - n$. Now, $m - n(q + 1) \leq r \leq 0$ which contradicts the fact that r is the smallest element of S. Therefore $0 \leq r \leq n - 1$ is true and which we can use to find both r and q.

□

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. We can create the assumption that q and r in the Division Algorithm are not unique.
Given q_1, q_2, r_1 and r_2 are integers and $q_1 \neq q_2$ and $r_1 \neq r_2$, we can then assume that:

$$nq_1 + r_1 = m = nq_2 + r_2 \qquad \text{with } 0 \leq r_1, r_2 \leq n-1$$

Then,

$$\begin{aligned} nq_1 + r_1 &= nq_2 + r_2 \\ n(q_1 - q_2) &= r_2 - r_1 \end{aligned}$$

Which suggests that $n|r_2 - r_1$. With the above inequalities we can deduce that

$$-n < r_2 - r_1 < n$$

This suggests that the only multiple of n is 0 so $r_2 - r_1 = 0 \iff r_2 = r_1$. this shows that r is unique. Consequently, we can deduce that $q_1 = q_2$ since $r_2 = r_1$ and $nq_1 + r_1 = nq_2 + r_2 = nq_1 + r_2 = nq_2 + r_1$. Thus both q and r are unique. □

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. By definition, $a \equiv b \pmod{n}$ can be expressed as $n|a-b \longleftrightarrow a - b = nk$ with $k \in \mathbb{Z}$ which can also be expressed as $a = nk + b$. this statement is similar to the division algorithm $m = nq + r$. This shows that b is the remainder when a is divided by n. Now, suppose r is r the remainder of b when divided by n $b = qn + r \iff b \equiv r \pmod{n}$ with $q \in \mathbb{Z}$:

$$\begin{aligned} a &= nk + b \\ a &= nk + (qn + r) && \text{(Substituting b)} \\ a &= n(k + q) + r \end{aligned}$$

Thus r is also the remainder of a, $a \equiv r \pmod{n}$. □

1.29 Question

Do every two integers have a least one common divisor?
Yes, each number can be divided by at least one common divisor which is 1. For example, prime numbers.

1.30 Question

Can two integers have infinitely many common divisors?
No, except for 0 and 0.

1.31 Exercise

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

1. (36, 22)

   $\gcd(36, 22) = 2$

2. (45, -15)

   $\gcd(45, -15) = 5$

3. (-296, -88)

   $\gcd(-296, -88) = 8$

4. (0, 256)

   $\gcd(0, 256) = 0$

5. (15, 28)

   $\gcd(15, 28) = 1$

6. (1, -2436)

   $\gcd(1, -2436) = 1$

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. By definition, $k|a$, $k|b$ and $k|r$ can be expressed as:

$$a = tk \qquad \text{where } t \in \mathbb{Z} \text{ and } t > 0$$

Similarly,

$$b = sk \qquad \text{where } s \in \mathbb{Z} \text{ and } s > 0$$

and

$$r = uk \qquad \text{where } u \in \mathbb{Z} \text{ and } u > 0$$

Substituting in $a = nb + r$:

$$\begin{aligned} a &= nb + r \\ tk &= n(sk) + r \\ tk - n(sk) &= r \\ (t - ns)k &= r \end{aligned}$$

Where $t - ns \in \mathbb{Z}$ and $t - ns > 0$ same as u in $r = uk$, thus satisfying $k|r$. □

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. By the Division Algorithm, we know that:

$$\begin{aligned} a &= n_1 b + r_1 \\ b &= n_1 r_1 + r^{'} \end{aligned}$$

This goes on until $0 \leq r^{'} \leq n_1 - 1$, which shows that if $(a, b) = r^{'}$ then $(b, r_1) = r^{'}$. □

1.34 Exercise

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

$$\begin{aligned} 51 &= 3 * 15 + 6 \\ 15 &= 2 * 6 + 3 \\ 6 &= 2 * 3 + 0 \end{aligned}$$

Thus 6 is the gcd$(51, 15)$ and since $3|6$ then $(51, 15) = (6, 3) = 3$.

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. Given (a,b), reorder a and b such that a is greater than b

1. Divide a with b, the result should give an approximation to n
2. Now guess an n with an r such that r is the smallest value possible but not 0.
3. Replace a with b and b with r until no further possibilities available or until the remainder is 0. Then the r right before the remainder was 0 is our gcd.

1.36 Exercise

Use the Euclidean Algorithm to find the gcd of

1. (96, 112) = 16

$$112 = 1 * 96 + 16$$
$$96 = 6 * 16 + 0$$

2. (162, 31) = 1

$$162 = 5 * 31 + 7$$
$$31 = 4 * 7 + 3$$
$$7 = 2 * 3 + 1$$
$$3 = 3 * 1 + 0$$

3. (0, 256)

$$256 = 0 * 0 + 256$$

Not possible

4. (-288, -166) = 2

$$-288 = 1 * -166 - 122$$
$$-166 = 1 * -122 - 44$$
$$-122 = 2 * -44 - 34$$
$$-44 = 1 * -34 - 10$$
$$-34 = 3 * -10 - 4$$
$$-10 = 2 * -4 - 2$$
$$-4 = 2 * -2 + 0$$

5. (1, -2436) = 1

$$-2436 = -2436 * 1 = 0$$

1.37 Exercise

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

Since x and y are integers they must satisfy:
$1 \equiv 162x \pmod{31}$
$1 \equiv 31y \pmod{162}$

We can find x by doing an multiplication inverse on 162 (mod 31) $\equiv$ 9. Then we can plug in x to find y which would be -47.

1.38 Theorem

Let a and b be integers. If (a, b) = 1, then there exist integers x and y such that $ax + by = 1$.

Proof. Using Euclidean Algorithm, we can demonstrate

$$a = n * b + 1$$
$$b = n_1 * 1 + 0$$

Substituting in $ax + by = 1$:

$$ax + by = 1$$
$$x(n * b + 1) + by = 1$$

Since x and y are integers they must satisfy:
$1 \equiv (n * b + 1)x \pmod{b}$
$1 \equiv by \pmod{(n * b + 1)}$

□

We can conclude that since both statements are true that there exists x and y such that $ax + by = 1$.

1.39 Theorem

Let a and b be integers. If there exist integers x and y with $ax + by = 1$*, then (a,b) = 1.*

Proof. Assume that $(a, b) = k \neq 1$. In this case we would have, $a = k * p$ and $b = k * q$ where p and q are some integers.
Lets evaluate $ax + by = 1$:

$$ax + by = 1$$
$$dpx + dqy = 1$$
$$d(px + qy) = 1$$

If we modulo each side to $\pmod{d}$:

- Left side: $d(px + qy) \pmod{d} \equiv 0$
- Right side: $1 \pmod{d} \equiv 1$

This is impossible if $d \neq 1$. Therefore, $(a, b) = 1$. □

1.40 Theorem (Bezout's Theorem)

For any integers a and b not both 0, there are integers x and y such that

$$ax + by = (a, b)$$

Proof. Given an assumption that $a \neq 0$. We can construct set S with the results of $ap + bq$ such that:

$$S = \{ap + bq\} \text{ with } ap + bq > 0 \text{ and } p, q \in \mathbb{Z}$$

The set is also non-empty since $|a| = ap + b * 0$ where $u \in \{-1, 1\}$ depending on the sign of a (negative or positive). By well-ordering principle, the set S must contain a least element, say u. That means that since $u \in S$, there must exist integers p and q such that $u = ap + bq > 0$. By the above claim, $u = \gcd(a, b)$. By the Division Algorithm, $a = n * u + r$ where $n, r \in \mathbb{Z}$ and $0 \leq r \leq u$. Assume $r \neq 0$:

$$0 < r = a - n * u = a - n * (ap + bq) = a - n * ap - n * bq = a(1 - np) + b(-nq)$$

Now considering our set S, the equation above implies that r is in S which contradicts the well-ordering principle that suggest that u is the smallest element in the set S. Thus, showing that $u|a$ and similarly $u|b$ by theorem 1.2 if $a - r = n * u$.
Thus since d divides both a and b, d = gcd(a,b). □

1.41 Exercise

Let a, b, and c be integers. If a|bc and (a,b) = 1, then a|c.

Proof. By definition, (a,b) = 1 implies that $ax + by = 1$ which we can then manipulate:

$$\begin{aligned} ax + by &= 1 \\ c(ax + by) &= c \qquad \text{(Multiplying c in both sides)} \\ acx + bcy &= c \end{aligned}$$

We can then assume that $a|a \implies a|acx$ and $a|bc \implies a|bcy$. By theorem 1.4, we can express $a|acx + bcy \implies a|c$ since $c = acx + bcy$. □

1.42 Theorem

Let a, b, and n be integers. If a|n, b|n and (a,b) = 1, then ab|n.

Proof. By definition, (a,b) = 1 can be expressed as $ax + by = 1$. $a|n \implies n = at, t \in \mathbb{Z}$, $b|n \implies n = bs, s \in \mathbb{Z}$ Also that With manipulation we can prove that

$ab|n$ with the following:

$$\begin{aligned} ax + by &= 1 && \\ n(ax + by) &= n && \text{(Multiplying n in both sides)} \\ anx + bny &= n && \\ (bs)ax + (at)by &= n && \text{(Substituing n with } bs \text{ and } at) \\ ab(sx + ty) &= n && \text{Where } sx + ty \in \mathbb{Z} \end{aligned}$$

Thus proving that $ab|n$. □

1.43 Theorem

Let a, b, and n be integers. If (a,n) = 1 and (b,n) = 1, then (ab, n) = 1.

Proof. By definition, $(a, n) = 1$ and $(b, n) = 1$ can be expressed as $(a, n) = 1 \implies at + ns = 1 \implies at = 1 - ns, \exists t, s \in \mathbb{Z}$ and $(b, n) = 1 \implies bu + nv = 1 \implies bu = 1 - nv, \exists u, v \in \mathbb{Z}$. By multiplying both equations, we get $at * bu$

$$\begin{aligned} (at)(bu) &= (1 - ns)(1 - nv) && \\ ab(tu) &= 1 - ns - nv - n^2sv && \\ ab(tu) &= 1 - n(s - v - nsv) && \\ ab(tu) + n(s - v - nsv) &= 1 && \\ ab(x) + n(s - v - nsv) &= 1 && (tu = x \text{ where } x \in \mathbb{Z}) \\ ab(x) + n(y) &= 1 && ((s - v - nsv) = y \text{ where } y \in \mathbb{Z}) \end{aligned}$$

Thus, by definition $ab(x) + n(y) = 1 \implies \gcd(ab, n) = 1$. □

1.44 Question

What hypothesis about a, b, c, and n could be added so that $ac \equiv bc \pmod{n}$ *would imply* $a \equiv b \pmod{n}$*?* The hypothesis implies that (c, n) = 1.

Proof. Suppose (c, n) = 1 then c is prime to n. Now, given $ac \equiv bc \pmod{n} \implies ac - bc = pn, p \in \mathbb{Z}$. Consequently,

$$\begin{aligned} ac - bc &= pn \\ c(a - b) &= pn \\ a - b &= \frac{pn}{c} \end{aligned}$$

Since, $a - b \in \mathbb{Z}$ then $\frac{pn}{c} \in \mathbb{Z}$ thus $c|pn$. Knowing that c is prime to n, $c|pn \implies c|p \implies p = cq, q \in \mathbb{Z}$. Now substituting p in $a - b = \frac{pn}{c} \implies a - b = qn$. Thus, $a \equiv b \pmod{n}$. □

1.45 Theorem

Let a, b, c and n be integers with $n > 0$. If $ac \equiv bc \pmod{n}$ and (c,n) = 1, then $a \equiv b \pmod{n}$.

Proof. Given that $(c, n) = 1$, this means that c is prime to n. With that in mind, $ac \equiv bc \pmod{n} \implies n|(ac - bc) \implies n|c(a - b)$. With c being prime to n, we c have $n|(a - b) \implies a \equiv b \pmod{n}$. □

1.46 Question

Suppose a, b, and c are integers and that there is a solution to the linear Diophantine equation

$$ax + by = c$$

that is, suppose there are integers x and y that satisfy the equation $ax + by = c$. What condition must c satisfy in terms of a and b?

The condition that must be satisfied is that $\gcd(a, b)|c$.

1.47 Question

Can you make a conjecture by completing the following statement?
Conjecture. *Given integers a, b, and c, there exist integers x and y that satisfy the equation $ax + by = c$ if and only if: $(a, b)|c$.*

1.48 Theorem

Given integers a, b, and c with a and b not both 0, there exist integers x and y that satisfy the equation $ax + by = c$ if and only if $(a, b)|c$.

Proof. If $(a, b)|c$ then $\gcd(a, b) * n = c, \exists n \in \mathbb{Z}$. Now by definition, $(a, b) = ax_1 + by_1, \exists x_1, y_1 \in \mathbb{Z}$. Suppose that $x_1 = x * n$ and $y_1 = y * n$. We know that $(a, b)|ax_1 \implies (a, b)|ax * n$ and $(a, b)|by_1 \implies (a, b)|by * n$. By theorem 1.1, $(a, b)|x_1 + y_1 \implies (a, b)|x * n + x * n \implies (a, b)|n(ax + by) \implies (a, b)|c$. □

1.49 Question

For integers a, b, and c, consider the linear Diophantine equation

$$ax + by = c$$

Suppose integers x_0 and y_0 satisfy the equation: that is, $ax_0 + by_0 = c$. What other values

$$x = x_0 + h \text{ and } y = y_0 + k$$

also satisfy $ax + by = c$? Formulate a conjecture that answers this question. Devise some numerical examples to ground your exploration. For example, $6(-3)+15*2 = 12$. Can you find other integers x and y such that $6x+15y = 12$? How many other pairs of integers x and y can you find? Can you find infinitely many other solutions?

Conjecture. *Given $x = x_0 + \frac{bn}{\gcd(a,b)}, \exists n \in \mathbb{Z}$, same goes for $y = y_0 - \frac{an}{\gcd(a,b)}$. Any integer value of n would result in an infinite number of solutions.*

Proof. Given that $ax + by = c, (a, b)|c$, $6x + 15y = 12, \gcd(6, 15)|12 \implies 3|12$. Using the Division Algorithm on this linear Diophantine, we can deduce:

$$\begin{aligned} 15 &= 6 * 2 + 3 \\ \implies 3 &= 15 - 6 * 2 \\ \implies 12 &= 15(4) - 6 * (8) \qquad \text{(Multiplying by 2 on each side)} \end{aligned}$$

Thus $x_0 = -8$ and $y_0 = 4$. Attempting solution with $x = x_0 + \frac{bn}{\gcd(a,b)}$ and $y = y_0 - \frac{an}{\gcd(a,b)}$

$$x = x_0 + \frac{bn}{\gcd(a, b)}$$
$$x = -8 + \frac{15n}{3}$$

$$y = y_0 - \frac{an}{\gcd(a, b)}$$
$$y = 4 - \frac{6n}{3}$$

With simple trial, we can see that all values for n work. □

1.50 Exercise (Euler).

A farmer lays out the sum of 1,770 crowns in purchasing horses and oxen. He pays 31 crowns for each horse and 21 crowns for each ox. What are possible numbers of horses and oxen that the farmer bought?

Let x = number of horses and y = number of oxen. The problem results into a Diophantine such as:

$$31x + 21y = 1770$$

Since $\gcd(31, 21) = 1$, then we can assume that $31x_0 + 21y_0 = 1, \exists x_0, y_0 \in \mathbb{Z}$. By Euclidean algorithm, we can find x_0 and y_0 to be:

$$\begin{aligned} 31x_0 + 21y_0 &= 1 \\ 31(-2) + 21(3) &= 1 \\ 31(-2 * 1770) + 21(3 * 1770) &= 1770 \end{aligned}$$

Hence, $x_0 = -2 * 1770$ and $y_0 = 3 * 1770$. Following the conjecture from the previous question, $x = -2 * 1770 + 21n$ and $y = 3 * 1770 - 31n$ for some $n \in \mathbb{Z}$. We can also approximate n by the following:
$-2 * 1770 + 21n \geq 0 \Rightarrow 21n \geq 2 * 1770 \Rightarrow n \geq \frac{2*1770}{21}$
$3 * 1770 - 31n \geq 0 \Rightarrow 3 * 1770 \geq 31n \Rightarrow \frac{3*1770}{31} \geq n$
Therefore, n can possibly be 169, 170 or 171. After re plugging back, we can arrive to the following solutions:
$(x, y) = (9, 71) = (30, 40) = (51, 9)$

1.51 Theorem

Let a, b, c, x_0, and y_0 be integers with a and b not both 0 such that $ax_0 + by_0 = c$. Then the integers

$$x = x_0 + \frac{b}{(a,b)} \text{ and } y = y_0 - \frac{a}{(a,b)}$$

also satisfy the linear Diophantine equation $ax + by = c$.

Proof. Assuming $x = x_0$ and $y = y_0$ are solution for $ax + by = c$.
Considering $x = x_0 + \frac{bn}{(a,b)}$ and $y = y_0 - \frac{an}{(a,b)}$ where for some $n \in \mathbb{Z}$ from the 1.49 Question. Now equating in $ax + by = c$:

$$\begin{aligned}
&\Rightarrow ax + by \\
&\Rightarrow a(x_0 + \frac{bn}{(a,b)}) + b(y_0 - \frac{an}{(a,b)}) \\
&\Rightarrow ax_0 + \frac{abn}{(a,b)} + by_0 - \frac{abn}{(a,b)} \\
&\Rightarrow ax_0 + by_0 + \frac{abn - abn}{(a,b)} \\
&\Rightarrow ax_0 + by_0 \\
&\Rightarrow c
\end{aligned}$$

□

Therefore, $x = x_0 + \frac{bn}{(a,b)}$ and $y = y_0 - \frac{an}{(a,b)}$ is a solution for $ax + by = c$.

1.52 Question

If a, b, and care integers with a and b not both 0, and the linear Diophantine equation

$$ax + by = c$$

has at least one integer solution, can you find a general expression for all the integer solutions to that equation?
Conjecture. *Given $x = x_0 + \frac{bn}{\gcd(a,b)}, \exists n \in \mathbb{Z}$, same goes for $y = y_0 - \frac{an}{\gcd(a,b)}$.*

Any integer value of n would result in an infinite number of solutions for $ax + by = c$.

Proof. Proof can be found in question 1.49. □

1.53 Theorem

Let a, b, and c be integers with a and b not both 0. If $x = x_0$, $y = y_0$ is an integer solution to the equation $ax + by = c$ (that is, $ax_0 + by_0 = c$) then for every integer k, the numbers

$$x = x_0 + \tfrac{kb}{(a,b)} \text{ and } y = y_0 - \tfrac{ka}{(a,b)}$$

are integers that also satisfy the linear Diophantine equation $ax+by = c$. Moreover, every solution to the linear Diophantine equation $ax + by = c$ is of this form.

Proof. Substituting into $ax + by = c$ and given that (a,b) = c:

$$\begin{aligned} ax + by &= c \\ a(x_0 + \frac{kb}{(a,b)}) + b(y_0 - \frac{ka}{(a,b)}) &= c \\ ax_0 + \frac{kab}{x} + by_0 - \frac{kab}{c} &= c \\ ax_0 + by_0 &= c \end{aligned}$$

Since x_0 and y_0 are integers, we can conclude that the proof is complete.

□

1.54 Exercise

Find all integer solutions to the equation $24x + 9y = 33$.

Possible solutions for x and y are $x = 1, y = 1$. From there, we can use the above theorem where $\gcd(24, 9) = 3$:

$$x = 1 + 3k \; y = 1 - 8k$$

Our results can vary depending on k.

1.55 Theorem

If a and b are integers, not both 0, and k is a natural number, then

$$\gcd(ka, kb) = k * \gcd(a, b).$$

Proof. Assume that $\gcd(a,b) = c$ and that $\gcd(ka,kb) = d$. Hence the theorem becomes $\gcd(ka,kb) = kc = k * \gcd(a,b) = d$.

$\Rightarrow \gcd(a,b) = c$
$\Rightarrow c|a$ and $c|b$
$\Rightarrow kc|ka$ and $kc|kb$ Multiplying each side with k
$\Rightarrow kc|\gcd(ka,kb) = d$
$\Rightarrow kc|d$

Also since $\gcd(a,b) = c$, using Theorem 1.48, $ax + by = c, \exists x,y \in \mathbb{Z} \Rightarrow k(ax + by) = kc.//$ Now since $\gcd(ka,kb) = d$:

$$\begin{aligned} &\Rightarrow \gcd(ka,kb) = d \\ &\Rightarrow d|ka \text{ and } d|kb \\ &\Rightarrow d|ka(x) + kb(y) \\ &\Rightarrow d|kc \end{aligned}$$

Since $kc|d$ and $d|kc$, we can then conclude that $kc = d$. □

1.56 Exercise

For natural numbers a and b, give a suitable definition for "least common multiple of a and b", denoted $lcm(a,b)$. Construct and compute some examples.

$$lcm(5,10) = min(5,10) = min10,20,30,40... = 10$$
$$lcm(24,26) = min(2 \cdot 2 \cdot 2 \cdot 3) \cup (2 \cdot 2 \cdot 3 \cdot 3) = 2$$

1.57 Theorem

If a and b are natural numbers, then $\gcd(a,b) \cdot lcm(a,b) = ab$.

Proof. Assume that a and b are divisible by c, $c|a$ and $c|b$. With that $a = cn, b = cm, \exists m,n \in \mathbb{Z}$ and also co-primes. Thus making lcm(m,n) with no common factors.
Now, if lcm(a,b) would be cmn and gcd(a,b) = c thus $\gcd(a,b) \cdot lcm(a,b) = c \cdot cmn = cm \cdot cn = ab$. □

1.58 Corollary

If a and b are natural numbers, then $lcm(a,b) = ab$ if and only if a and b are relatively prime.

Proof. If a and are not relative primes then $gcd(a,b) = c > 1$.
Since $\gcd(a,b) \cdot lcm(a,b) = ab \Rightarrow abc \neq ab$. Thus a and b must be relative primes so gcd(a,b) = 1. □

1.59 Blank Paper Exercise

- Divides notation $n|a \Rightarrow a = kn, \exists k \in \mathbb{Z}$
- Induction Proofs
- Congruence and Modulo calculation
- Division Algorithm
- Greatest Common Divisor
- Least Common Divisor
- Diophantine Equations and uses for relative primes
- Euclidean Algorithm and the Euler farmer problem
- multiple solution for x and y for $ax + by = c, (a, b) = c$

Most difficult part was formulating proofs using other proofs instead of derving equations.