Foundations Homework 4

TJ Liggett

25 September 2019

Chapter Two

Assignment 6 *Prove the Fundamental Theorem of Arithmetic by showing that there is no smallest natural number with multiple prime factorizations.*

Assume, by way of contradiction, there exists a smallest natural number with multiple prime factorizations: $N = p_1p_2...p_m = q_1q_2...q_n$. Then there are two cases, one where the factorizations share a prime in common, and one where they do not.

1. Assume the factorizations share a prime in common. Then there exists a number $p_k = q_k = n$ where n divides both factorizations. However, this would imply there exists a number smaller than N which has multiple prime factorizations, which is a contradiction.

2. Assume the factorizations share no primes in common, so $p_1 \neq q_1$. Without loss of generality, assume $p_1 < q_1$. So $p_1 + \delta = q_1$ for some δ. Let $P = p_2...p_m, Q = q_1q_2...q_n$. Because $p_1 < q_1$, it follows that $Q < P$, and $Q + \Delta = P$. Observe that
$$M = \delta P = (q_1 - p_1)P = q_1P - N = q_1(P - Q) = q_1\Delta \tag{1}$$
Because $M = \delta P = q_1\Delta$, M is a number with two unique prime factorizations. However, since $\Delta < Q$, it is true that $M < N$, which is a contradiction.

Therefore, by way of contradiction, the Fundamental Theorem of Arithmetic is true.

Assignment 8 *Prove that for natural numbers m, n, and k,*

1. $(km, kn) = k(m, n)$,

2. $[km, kn] = k[m, n]$,

PROOF 1 Let m, n, k be natural numbers. Then the exponent vector of (km, kn) is:

$$(min(k_1m_1, k_1n_1), min(k_2m_2, k_2n_2), ..., min(k_jm_j, k_jn_j)) \tag{2}$$

For any natural numbers $k_i m_i$ and $k_i n_i$, $min(k_i m_i, k_i n_i) = k_i * min(m_i, n_i)$. Thus,

$$(min(k_1m_1, k_1n_1), min(k_2m_2, k_2n_2), ..., min(k_jm_j, k_jn_j)) \tag{3}$$

$$= (k_1 min(m_1, n_1), k_2 min(m_2, n_2), ..., k_j min(m_j, n_j)) \tag{4}$$

$$= (k_1, k_2, ..., k_j)(min(m_1, n_1), min(m_2, n_2), ..., min(m_j, n_j)) = k(m, n) \tag{5}$$

Therefore, $(km, kn) = k(m, n)$.

PROOF 2 Let m, n, k be natural numbers. Then the exponent vector of $[km, kn]$ is:

$$(max(k_1m_1, k_1n_1), max(k_2m_2, k_2n_2), ..., max(k_jm_j, k_jn_j)) \tag{6}$$

For any natural numbers $k_i m_i$ and $k_i n_i$, $max(k_i m_i, k_i n_i) = k_i * max(m_i, n_i)$. Thus,

$$(max(k_1m_1, k_1n_1), max(k_2m_2, k_2n_2), ..., max(k_jm_j, k_jn_j)) \tag{7}$$

$$= (k_1 max(m_1, n_1), k_2 max(m_2, n_2), ..., k_j max(m_j, n_j)) \tag{8}$$

$$= (k_1, k_2, ..., k_j)(max(m_1, n_1), max(m_2, n_2), ..., max(m_j, n_j)) = k[m, n] \tag{9}$$

Therefore, $[km, kn] = k[m, n]$.

Assignment 9 *State and prove a theorem concerning the product* $(m, n)[m, n]$.

If m,n are natural numbers, then

$$(m, n)[m, n] = mn \tag{10}$$

Let m, n be natural numbers, and m and n have exponent vectors equal to $(m_1, m_2, ..., m_k)$ and $(n_1, n_2, ..., n_k)$. Since (m, n) has an exponent vector of all the lower components of m and n exponent vectors, and $[m, n]$ has an exponent vector containing all of the higher components, it follows that the exponent vector for $(m, n)[m, n]$ is equal to $(m_1 + n_1, m_2 + n_2, ..., m_k + n_k)$, which is the exponent vector for mn. Therefore, $(m, n)[m, n] = mn$.

Exercise 10 *Let* $m = 5$. *Complete the following:*

(a) $8 \equiv \_\_ \pmod{m}$,

(b) $12 \equiv \_\_ \pmod{m}$,

(c) $(8 + 12) \equiv \_\_ \pmod{m}$,

(d) $8 * 12 \equiv \_\_ \pmod{m}$

Let m = 5. Then:

(a) $8 \equiv 3 \pmod{m}$,

(b) $12 \equiv 2 \pmod{m}$,

(c) $(8 + 12) \equiv 0 \pmod{m}$,

(d) $8 * 12 \equiv 1 \pmod{m}$

Exercise 11 *Repeat the preceding exercise with $m = 6$.*

Let m = 6. Then:

(a) $8 \equiv 2 \pmod{m}$,

(b) $12 \equiv 0 \pmod{m}$,

(c) $(8 + 12) \equiv 2 \pmod{m}$,

(d) $8 * 12 \equiv 0 \pmod{m}$

Assignment 12 *Let $k > n$. Show that k and n are congruent modulo m iff $m|(k-n)$.*

First, let us prove that if k and n are congruent modulo m, then $m|(k-n)$. Assume k and n are congruent modulo m, and thus there are natural numbers $q_1, q_2, andr$ such that $r < m$ and $k = q_1m + r$ and $n = q_2m + r$. Then,

$$k - n = (q_1m + r) - (q_2m + r) = q_1m - q_2m = (q_1 - q_2)m \tag{11}$$

Since $k > n$, $(q_1 - q_2)$ is a natural number, and it follows that $m|k - n$.

Now, let us prove that if $m|(k-n)$, then k and n are congruent modulo m. Assume $m|(k-n)$. Then, $k - n = jm$ for some natural number, and thus $k = jm + n$. Consider the two cases, where (1) $m|n$ or (2) $m \not| n$.

1. Assume $m|n$. Then $n = am$ for some natural number a. Thus, $k = jm + am = m(j + a)$. Since the natural numbers are closed under addition, it follows that $m|k$. Since $m|n, k$, k and n are congruent modulo m.

2. Assume $m \not| n$. Then $n = am + r$ for some natural numbers a, r where $r < m$. It follows that $k = jm + am + r = m(j + a) + r$. Since the natural numbers are closed under addition, it follows that k and n are congruent modulo m with the same remainder r.

Therefore, k and n are congruent modulo m iff $m|(k-n)$.

Assignment 13 *Let $a, b, c, d, s, t, k, andm$ denote natural numbers. Then*

1. *$a \equiv b \pmod{m}$, $b \equiv a \pmod{m}$, and $|a-b| \equiv 0 \pmod{m}$ are logically equivalent statements.*
2. *If $a \equiv b \pmod{m}$ and $b \equiv c \pmod{m}$, then $a \equiv c \pmod{m}$.*
3. *If $a \equiv b \pmod{m}$ and $c \equiv d \pmod{m}$, then $as + ct \equiv bs + dt \pmod{m}$.*
4. *If $a \equiv b \pmod{m}$ and $c \equiv d \pmod{m}$, then $ac \equiv bd \pmod{m}$.*
5. *If $a \equiv b \pmod{m}$, then $ak \equiv bk \pmod{m}$ for every k.*
6. *If $a \equiv b \pmod{m}$ and $d|m$, then $a \equiv b \pmod{d}$.*

PROOF 1

Observe that if $a \equiv b \pmod{m}$, then $a = q_1 m + r$, $b = q_2 m + r$ for some natural numbers q_1, q_2, r where $r < m$. By definition, it follows that $b \equiv a \pmod{m}$. Likewise, if $b \equiv a \pmod{m}$, $a \equiv b \pmod{m}$ through the same logic. By Assignment 2.12, if $a \equiv b \pmod{m}$, then $m|(a-b)$. By the definition of divides, $\frac{a-b}{m}$ has a remainder of 0. This is equivalent to saying $|a-b| \equiv 0 \pmod{m}$, as the difference between a and b will have a remainder of 0 when divided by m. Therefore, $a \equiv b \pmod{m}$, $b \equiv a \pmod{m}$, and $|a-b| \equiv 0 \pmod{m}$ are logically equivalent statements.

PROOF 2

Let a, b, c, m be natural numbers, where $a \equiv b \pmod{m}$ and $b \equiv c \pmod{m}$. Then,

$$a = q_1 m + r, b = q_2 m + r, b = q_3 m + s, c = q_4 m + s \tag{12}$$

Where q_1, q_2, q_3, q_4, r, s are natural numbers and $r, s < m$. It follows that:

$$b = q_2 m + r = q_3 m + s \tag{13}$$

$$r = q_3 m - q_2 m + s \tag{14}$$

$$a = q_1 m + r = q_1 m + q_3 m - q_2 m + s = (q_1 + q_3 - q_2) m + s \tag{15}$$

Since $a = (q_1 + q_3 - q_2)m + s$, $c = q_4 m + s$, and $(q_1 + q_3 - q_2)$ is a positive natural number, $a \equiv c \pmod{m}$.

Therefore, if $a \equiv b \pmod m$ and $b \equiv c \pmod m$, then $a \equiv c \pmod m$.

PROOF 3

Let a, b, c, d, m, s, t be natural numbers where $a \equiv b \pmod m$ and $c \equiv d \pmod m$. Then,

$$a = q_1 m + r, b = q_2 m + r, c = q_3 m + p, d = q_4 m + p \tag{16}$$

Where q_1, q_2, q_3, q_4, r, p are natural numbers and $r, p < m$. It follows that:

$$as + ct = (q_1 m + r)s + (q_3 m + p)t = q_1 ms + rs + q_3 mt + pt \tag{17}$$

$$bs + dt = (q_2 m + r)s + (q_4 m + p)t = q_2 ms + rs + q_4 mt + pt \tag{18}$$

Since s, t are natural numbers, it follows that $rs = q_5 m + x$ and $pt = q_6 m + y$ for some natural numbers q_5, q_6, x, y where $x, y < m$. So,

$$as + ct = q_1 ms + q_5 m + x + q_3 mt + q_6 m + y = (q_1 s + q_5 + x + q_3 t + q_6)m + x + y \tag{19}$$

$$bs + dt = q_2 ms + q_5 m + x + q_4 mt + q_6 m + y = (q_2 s + q_5 + x + q_4 t + q_6)m + x + y \tag{20}$$

By definition, it follows that $as + ct \equiv bs + dt \pmod m$.
Therefore, if $a \equiv b \pmod m$ and $c \equiv d \pmod m$, then $as + ct \equiv bs + dt \pmod m$.

PROOF 4

Let a, b, c, d, m be natural numbers, where $a \equiv b \pmod m$ and $c \equiv d \pmod m$. Then,

$$a = q_1 m + r, b = q_2 m + r, c = q_3 m + s, d = q_4 m + s \tag{21}$$

Where q_1, q_2, q_3, q_4, r, s are natural numbers and $r, s < m$. It follows that:

$$ac - bd = (q_1 m + r)(q_3 m + s) - (q_2 m + r)(q_4 m + s) \tag{22}$$

$$= (q_1 q_3 m^2 + q_1 ms + q_3 mr + rs) - (q_2 q_4 m^2 + q_2 ms + q_4 mr + rs) \tag{23}$$

$$= m(q_1 q_3 m + q_1 s + q_3 r - q_2 q_4 m + q_2 s + q_4 r) \tag{24}$$

Since $(q_1 q_3 m + q_1 s + q_3 r - q_2 q_4 m + q_2 s + q_4 r)$ is an integer, it follows that $m | ac - bd$. Thus, by Assignment 2.12, $ac \equiv bd \pmod m$.

Therefore, if $a \equiv b \pmod{m}$ and $c \equiv d \pmod{m}$, then $ac \equiv bd \pmod{m}$.

PROOF 5

Let a, b, k, m be natural numbers where $a \equiv b$ (mod m). By Assignment 2.12, $m|(a-b)$. It follows that, for some natural number q,

$$a - b = mq \tag{25}$$

$$k(a-b) = kmq \tag{26}$$

$$ak - bk = (kq)m \tag{27}$$

Since the natural numbers are closed under multiplication and adhere to the associative property, then $m|(ak - bk)$. Thus, by Assignment 2.12, $ak \equiv bk \pmod{m}$. Therefore, if $a \equiv b \pmod{m}$, then $ak \equiv bk \pmod{m}$ for every k

PROOF 6

Let a, b, d, m be natural numbers, where $a \equiv b$ (mod m) and $d|m$. Then $a = q_1m + r$, $b = q_2m + r$, and $m = kd$ where q_1, q_2, r, k are natural numbers with $r < m$. It follows that:

$$a = q_1m + r = (q_1k)d + r \tag{28}$$

$$b = q_2m + r = (q_2k)d + r \tag{29}$$

Since natural numbers are closed under multiplication, $a = q_3d+r$ and $b = q_4d+r$ for some natural numbers q_3 and q_4. Thus, by definition, $a \equiv b \pmod{d}$.

Therefore, if $a \equiv b \pmod{m}$ and $d|m$, then $a \equiv b \pmod{d}$.