MAT2120 Number Theory
Homework, September 26th

Suhyun Park (20181634)

Department of Computer Science and Engineering, Sogang University

Theorem 1. *For* $a > 0, b > 0 \in \mathbb{Z}$*,*

$$(a, b)\,[a, b] = ab.$$

Lemma 1. *For* $k > 0 \in \mathbb{Z}$*,* $[ka, kb] = k\,[a, b]$.

Proof. Since $ka \mid [ka, kb]$, $k \mid [ka, kb]$.

Let $l = [a, b]$ and $km = [ka, kb]$. Then

$$ka \mid km \Rightarrow a \mid m \qquad \text{and} \qquad kb \mid km \Rightarrow b \mid m.$$

Hence m is a common multiple of a and b, giving that

$$m \geq l \tag{1}$$

because l is the least common multiple of a and b.

Similarly,

$$a \mid l \Rightarrow ka \mid kl \qquad \text{and} \qquad b \mid l \Rightarrow kb \mid kl.$$

Hence kl is a common multiple of ka and kb, giving that

$$kl \geq km \Rightarrow l \geq m \tag{2}$$

because km is the least common multiple of ka and kb.

By (1) and (2), we can conclude that $l = m$. Therefore

$$[ka, kb] = km = kl = k[a, b].$$

□

Proof (Conclusion of Proof of Theorem). Let $d = (a, b)$. Then $d \mid a$ and $d \mid b$ is true by definition.

Hence we let $a = a_0 d$, $b = b_0 d$. Then $(a_0, b_0) = 1$.

Now we want to show that $[a_0, b_0] = a_0 b_0$. Since $a_0 \mid [a_0, b_0]$, we let $[a_0, b_0] = k a_0$.

Since $b_0 \mid [a_0, b_0] \Rightarrow b_0 \mid k a_0$ and $(a_0, b_0) = 1$, we know that $b_0 \mid k$. Thus, $b_0 a_0 \leq k a_0$.

Note that $k a_0$ is the least common multiple of a_0, b_0 and $b_0 a_0$ is the common multiple of a_0, b_0, thus $b_0 a_0 \geq k a_0$. Hence $a_0 b_0 = k a_0 = [a_0, b_0]$.

Using Lemma 1, we can conclude that

$$\begin{aligned} & (a, b)[a, b] \\ =& d[a_0 d, b_0 d] \\ =& d^2 [a_0, b_0] \\ =& d^2 a_0 b_0 = (d a_0)(d b_0) \\ =& ab. \end{aligned}$$

□

Theorem 2. *Let b be a positive integer with $b > 1$. Then every positive integer n can be expressed in unique form of*

$$n = a_k b^k + a_{k-1} b^{k-1} + \cdots + a_1 b^1 + a_0$$

where $a_i \in \mathbb{Z}$, $0 \leq a_i \leq b - 1$ for $i = 0, 1, \cdots, k$ and $a_k \neq 0$.

Proof. We use the division algorithm. For $0 \leq a_0 < b$, we can express n as

$$n = q_0 b + a_0.$$

If $q_0 \geq b$, we can express q_0 as

$$q_0 = q_1 b + a_1.$$

We can repeat this process for q_i while $q_i \geq b$. This gives

$$\begin{aligned} n &= q_0 b^1 + a_0 \\ &= q_1 b^2 + a_1 b^1 + a_0 \\ &\vdots \\ &= a_k b^k + a_{k-1} b^{k-1} + \cdots + a_1 b^1 + a_0. \end{aligned}$$

Now we want to show that such $a_0, a_1, \cdots, a_k$ uniquely exists. Let

$$n = a'_k b^k + a'_{k-1} b^{k-1} + \cdots + a'_1 b^1 + a'_0.$$

Then

$$\begin{aligned} a_k b^k + a_{k-1} b^{k-1} + \cdots + a_1 b^1 + a_0 &= a'_k b^k + a'_{k-1} b^{k-1} + \cdots + a'_1 b^1 + a'_0 \\ \Rightarrow q_0 b^1 + a_0 &= q'_0 b^1 + a'_0. \\ \Rightarrow \left(q_0 - q'_0\right) b^1 &= a'_0 - a_0. \end{aligned}$$

If $q_0 \neq q'_0$, $b \mid (a'_0 - a_0)$, but since $0 \leq a_0, a'_0 < b$, $-b < a'_0 - a_0 < b$, which falls into contradiction. Hence $q_0 = q'_0$ and also $a_0 = a'_0$. Similarlily we can repeat this process for q_i to show that $a_i = a'_i$ for $0 \leq i \leq k$, proving that $a_0, a_1, \cdots, a_k$ uniquely exists. $\square$