Arkansas Tech University
MATH 4033: Elementary Modern Algebra
Dr. Marcel B. Finan

13 Least Common Multiple. The Fundamental Theorem of Arithmetic

In the previous section, we learned how to find the largest positive divisor of two integers that are not both zero. In this section, we want to find the smallest common factor of two nonzero integers, known as the **least common multiple**.
Finding least common multiples is useful in combining algebraic fractions. For example, to add the fractions $\frac{5}{2}+\frac{4}{3}+\frac{7}{4}$ one finds the common denominator which is the least common multiple of the integers $2, 3$, and 4. In this case, it is 12.

The following theorem establishes the existence of the least common multiple.

Theorem 13.1
If a and b are nonzero integers then there is a unique positive integer m such that

(1) $a|m$ and $b|m$;
(2) if c is an integer such that $a|c$ and $b|c$ then $m|c$.

Proof.
We first prove uniqueness. Suppose n and m are two positive integers that satisfy (1) and (2). Since m is a common multiple of a and b and since n satisfies (2) then $n|m$. Interchange the letters n and m to obtain $m|n$. By Theorem 10.4(d), $n = m$.
To prove existence, let $S = \{x \in \mathbb{N} : a|x \; and \; b|x\}$. Since $a|\ |ab|$ and $b|\ |ab|$ then $|ab| \in S$ and therefore $S \neq \emptyset$. By Theorem 10.1, S has a smallest element m. Thus, $a|m$ and $b|m$. This proves (1).
To prove (2), we assume that c is an integer such that $a|c$ and $b|c$. By the Division Algorithm there exist unique integers q and r such that

$$c = mq + r, \quad 0 \leq r < m.$$

Since $a|c$ then $c = aq_1$ for some $q_1 \in \mathbb{Z}$. Since $a|m$ then $m = aq_2$ for some $q_2 \in \mathbb{Z}$. Thus,

$$aq_1 = aqq_2 + r$$

or $a(q_1 - qq_2) = r$. This implies that $a|r$. A similar argument with b replacing a we find that $b|r$. If $r > 0$ then $r \in S$ and this contradicts the definition of m. So we must have $r = 0$. Therefore, $c = mq$ and $m|c$. This completes a proof of the theorem.■

Definition 13.1
According to (1), m is a common multiple of both a and b. By (2), m is the least such commom multiple. We call the positive integer m the **least common multiple** of a and b and we will denote it by $lcm(a, b)$.

Example 13.1
If $a = 25$ and $b = 33$ then $lcm(25, 33) = 825$. Similarly, $lcm(4, -6) = 12$.■

Our next goal is to find a method for finding the least common multiple of two nonzero integers. The method is a result of the **Fundamental Theorem of Arithmetic,** known also as the **Unique Factorization Theorem**.
In order to prove this theorem, one needs the following lemmas.

Lemma 13.1
If a, b, and c are integers such that $a|bc$ and $gcd(a, b) = 1$ then $a|c$.

Proof.
Since $gcd(a, b) = 1$ then by Theorem 12.4, there are integers m and n such that $ma + nb = 1$. Multiply this equation by c to obtain $mac + nbc = c$. Since $a|bc$ and $a|ac$ then $a|mac$ and $a|nbc$ (Theorem 10.2(a)). By Theorem 10.2(b), $a|\ (mac + nbc)$. That is, $a|c$. ■

Remark 13.1
The condition $gcd(a, b) = 1$ is critical. For example, if $a = 6, b = 3$, and $c = 4$. Then $a|bc$ but neither a divides b or a divides c. Note that $gcd(a, b) = 3 \neq 1$.

Lemma 13.2
If a is an integer and p is a prime number such that $p \not| a$ then $gcd(a, p) = 1$.

Proof.
Let $d = gcd(a, p)$. Then $d|a$ and $d|p$. Since p is prime then either $d = 1$ or $d = p$. If $d = p$ then $p|a$ which contradicts the fact that $p \not| a$. Thus, $d = 1$. ■

Lemma 13.3
If $a_1, a_2, \cdots, a_n$ are integers and p is a prime such that $p|\ a_1 a_2 \cdots a_n$ then $p|\ a_i$ for some $1 \leq i \leq n$.

Proof.
The proof is by induction on n. The case $n = 1$ is trivial. So assume that the lemma holds for all positive integers up to and including n-1. We will show that the result still holds for n. Since $p|\ a_1 a_2 \cdots a_n$ then either $p|a_1 a_2 \cdots a_{n-1}$ or $p\ \not|a_1 a_2 \cdots a_{n-1}$. If $p|\ a_1 a_2 \cdots a_{n-1}$ then by the induction hypothesis, $p|\ a_i$ for some $1 \leq i \leq n-1$. If $p\ \not|a_1 a_2 \cdots a_{n-1}$ then by Lemma 13.2, $gcd(p, a_1 a_2 \cdots a_{n-1}) = 1$. By Lemma13.1 (with $a = a_1 a_2 \cdots a_{n-1}$ and $b = a_n$) we have $p|a_n$. ■

Theorem 13.2 *(The Fundamental Theorem of Arithmetic)*
Every positive integer $n > 1$ is either a prime or can be written as a product of prime integers, and this product is unique except for the order of the factors.

Proof.
The proof is by induction on n. The statement of the theorem is trivially true for $n = 2$ since 2 is prime. Assume, then, that the statement of the theorem is true for the integers $2, 3, \cdots, n-1$. We shall prove it to be true for n. If n is prime there is nothing to prove. Assume, then, that n is composite. In this case, n is the product of positive integers with each factor less than n. By the induction hypothesis, each factor can be written as a product of prime numbers. Hence, n can be written as a product of prime numbers.
Now, assume that n has two factorizations, say

$$n = p_1 p_2 \cdots p_s = q_1 q_2 \cdots q_t \tag{1}$$

Since p_1 divides the product $q_1, q_2, \cdots, q_t$, then by Lemma 13.3, it must divide at least one factor. Relabel $q_1, q_2, \cdots, q_t$ so that $p_1|\ q_1$. Then $p_1 = q_1$ since both p_1 and q_1 are primes. In (1), we may cancel p_1 on both sides to obtain

$$\frac{n}{p_1} = p_2 p_3 \cdots p_s = q_2 q_3 \cdots q_t < n.$$

But $\frac{n}{p_1} \in \{2, 3, \cdots, n-1\}$ so that by the induction hypothesis, the two factorizations of $\frac{n}{p_1}$ must be identical except for the order of the factors. Therefore, $s = t$ and the factorizations in (1) are also identical, except for the order of factors. This ends a proof of the theorem.■

Remark 13.2
In the factorization of an integer $n > 1$, a particular prime p may occur more than once. If the distinct prime factors of n are $p_1 < p_2 < \cdots < p_s$ and if p_i occurs as a factor k_i times, we can write

$$n = p_1^{k_1} p_2^{k_2} \cdots p_s^{k_s}$$

We shall call this the **standard form** for n.

Lemma 13.4
Let m and n be two integers with the following prime factorization

$$m = p_1^{k_1} p_2^{k_2} \cdots p_s^{k_s} \quad and \quad n = p_1^{t_1} p_2^{t_2} \cdots p_s^{t_s}$$

Then $m|n$ if and only if $k_i \leq t_i$ for $1 \leq i \leq s$.

Proof.
If p is a prime and a and b are integers such that α is the highest power of p dividing a and β is the highest power of p dividing b then $a = p^\alpha q$ and $b = p^\beta q'$ for some $q, q' \in \mathbb{Z}$. Thus, $ab = p^{\alpha+\beta} q"$, where $q" \in \mathbb{Z}$. Hence, $\alpha + \beta$ is the highest power of p dividing ab. So if $m|n$ then $n = mu$ for some integer u. Thus, for each $1 \leq i \leq s$, the highest power of p_i dividing n is the sum of the highest powers of p_i dividing m and u. Thus, $k_i \leq t_i$ for $1 \leq i \leq s$.
Conversely, suppose that $k_i \leq t_i$ for all $1 \leq i \leq s$. Let $u_i = t_i - k_i$ for $1 \leq i \leq s$. Define $w = p_1^{u_1} p_2^{u_2} \cdots p_s^{u_s}$. Then $n = mw$ and so $m|n$.■

We have the following result which expresses $gcd(a, b)$ and $lcm(a, b)$ in terms of the factorizations of a and b.

Theorem 13.3
If two nonzero integers a and b have the factorizations

$$a = p_1^{k_1} p_2^{k_2} \cdots p_s^{k_s} \quad and \quad b = p_1^{t_1} p_2^{t_2} \cdots p_s^{t_s}$$

then

$$lcm(a, b) = p_1^{u_1} p_2^{u_2} \cdots p_s^{u_s}$$

where u_i is the maximum of k_i and t_i for each $1 \leq i \leq s$, and

$$gcd(a, b) = p_1^{v_1} p_2^{v_2} \cdots p_s^{v_s}$$

where v_i is the minimum of k_i and t_i for each $1 \leq i \leq s$.

Proof.
Let $m = p_1^{u_1} p_2^{u_2} \cdots p_s^{u_s}$ where u_i is the maximum of k_i and t_i. We will show that $m = lcm(a, b)$. Since $k_i \leq u_i$ and $t_i \leq u_i$ for all $1 \leq i \leq s$ then by Lemma 13.4, $a|m$ and $b|m$. Now, if c is an integer such that $a|c$ and $b|c$. Write $c = p_1^{w_1} p_2^{w_2} \cdots p_s^{w_s}$. Then by Lemma 13.4, $k_i \leq w_i$ and $t_i \leq w_i$ for all $1 \leq i \leq s$. Thus, $u_i \leq w_i$ for all $1 \leq i \leq s$. By Lemma 13.4, $m|c$. It follows that $m = lcm(a, b)$.
Let $m = p_1^{u_1} p_2^{u_2} \cdots p_s^{u_s}$ where u_i is the minimum of k_i and t_i. We will show that $m = gcd(a, b)$. Since $u_i \leq k_i$ and $u_i \leq t_i$ for all $1 \leq i \leq s$ then by Lemma 13.4, $m|a$ and $m|b$. Now, let c be an integer such that $c|a$ and $c|b$. Write $c = p_1^{w_1} p_2^{w_2} \cdots p_s^{w_s}$. Then by Lemma 13.4, $k_i \leq w_i$ and $t_i \leq w_i$ for all $1 \leq i \leq s$. Thus, $u_i \leq w_i$ for all $1 \leq i \leq s$. By Lemma 13.4, $c|m$. It follows that $m = gcd(a, b)$. ■

Remark 13.3
The above theorem gives a way to find $gcd(a, b)$ if we know the factorizations of a and b. But factorizing a number is a very hard problem and so, the above method is ineffective. Instead, the Euclidean Algorithm is more practical.

Example 13.2
Consider the prime factorizations of the integers 31752 and 126000 :

$$31752 = 2^3 \cdot 3^4 \cdot 7^2 \quad and \quad 126000 = 2^4 \cdot 3^2 \cdot 5^3 \cdot 7.$$

Then from Theorems 13.3 and **??** we have

$$lcm(31752, 126000) = 2^4 \cdot 3^4 \cdot 5^3 \cdot 7^2 = 7938000$$

and

$$gcd(31752, 126000) = 2^3 \cdot 3^2 \cdot 7 = 504.$$ ■

Corollary 13.1
If two nonzero integers a and b have the factorizations

$$a = p_1^{k_1} p_2^{k_2} \cdots p_s^{k_s} \quad and \quad b = p_1^{t_1} p_2^{t_2} \cdots p_s^{t_s}$$

then

$$lcm(a, b) gcd(a, b) = ab.$$

Proof.
First, note that $k_i + t_i = \max\{k_i, t_i\} + \min\{k_i, t_i\}$ for $1 \leq i \leq s$. Thus,

$$\begin{aligned} ab &= (p_1^{k_1} p_2^{k_2} \cdots p_s^{k_s}) \cdot (p_1^{t_1} p_2^{t_2} \cdots p_s^{t_s}) \\ &= p_1^{k_1+t_1} \cdot p_2^{k_2+t_2} \cdots p_s^{k_s+t_s} \\ &= (p_1^{u_1} p_2^{u_2} \cdots p_s^{u_s}) \cdot (p_1^{v_1} p_2^{v_2} \cdots p_s^{v_s}) \\ &= lcm(a,b)gcd(a,b) \blacksquare \end{aligned}$$

We have seen in the previous section that $\mathbb{Z}_n^*$ under $\odot$ is a group when n is prime. We will next consider subsets U_n of $\mathbb{Z}_n^*$ such that U_n is a group with respect to $\odot$ for any positive integer n, not necessarily prime.

Theorem 13.4
For each positive integer n let

$$U_n = \{[k] : 1 \leq k < n \ \ and \ \ gcd(k,n) = 1\}.$$

Then $(U_n, \odot)$ is an Abelian group.

Proof.
We will show that U_n is a subgroup of $\mathbb{Z}_n^*$. Since $[1] \in U_n$ then $U_n \neq \emptyset$. Now, let $[a], [b] \in U_n$. We will show that $[a] \odot [b] \in U_n$ Since $[a], [b] \in U_n$ then $gcd(a,n) = 1$ and $gcd(b,n) = 1$. By Theorem 12.4, there exist integers r, s, t, u such that $ar + ns = 1$ and $bt + nu = 1$. Thus, $(ar + ns)(bt + nu) = 1$ or

$$ab(rt) + n(aru + sbt + nsu) = 1.$$

By Theorem 12.4, $gcd(ab, n) = 1$). Thus, $[a] \odot [b] = [ab] \in U_n$.
Next, we will show that every element $[a] \in U_n$ is invertible. Indeed, since $[a] \in U_n$ then $gcd(a,n) = 1$ and by Theorem 12.4, there exist integers r and s such that $ar + ns = 1$. Thus, $ar - 1 = n(-s)$ and this implies that $ar \equiv 1 (mod\ n)$. Hence, $[a] \odot [r] = [1]$ and so $[a]$ is invertible. By Theorem 7.3, U_n is a subgroup and hence a group. Since $(Z_n^*, \odot)$ is Abelian so is $(U_n, \odot)$.$\blacksquare$

How many elements does U_n have? To answer this question, we introduce the following function.

Definition 13.2
For each positive integer n, let $\phi(n)$ denote the number of positive integers that are less than n and relatively prime to n. We define $\phi(1) = 1$. The function ϕ is called the **Euler phi function.**

Example 13.3
Find $\phi(5), \phi(6)$, and $\phi(12)$.

Solution.
From the above definition we have $\phi(5) = 4, \phi(6) = 2$, and $\phi(12) = 4$.■

Remark 13.4
By the above definition, it follows that $|U_n| = \phi(n)$.

Next, we discuss some properties of ϕ.

Theorem 13.5
For any prime number p and positive integer r we have

$$\phi(p^r) = p^r - p^{r-1}.$$

In particular, for $r = 1$ we have $\phi(p) = p - 1$.

Proof.
Let k be an integer such that $1 \leq k < p^r$. If $p|k$ then $gcd(k, p^r) \neq 1$. Hence, $gcd(k, p^r) = 1$ if and only if $p \not| k$. Now, if $p|k$ then $k \in \{p, 2p, 3p, \cdots, (p^{r-1} - 1)p\}$. Indeed, if $p|k$ then $k = pt$ for some positive integer t. But $k < p^r$ so that $pt < p^r$ and hence $t < p^{r-1}$. Thus, there are $p^{r-1} - 1$ positive integers less than p^r and divisible by p. The total number of integers less than p^r is $p^r - 1$. Thus, the number of integers less than p^r and not divisible by p, (i.e. relatively prime to p^r) is $p^r - 1 - (p^{r-1} - 1) = p^r - p^{r-1}$. That is, $\phi(p^r) = p^r - p^{r-1}$.■

Theorem 13.6
If p and q are relatively prime then $\phi(pq) = \phi(p)\phi(q)$.

Proof.
Let p and q be relatively prime integers. Write the numbers 1 to pq as an array

$$\begin{array}{ccccc} 1 & q+1 & 2q+1 & \cdots & (p-1)q+1 \\ 2 & q+2 & 2q+2 & \cdots & (p-1)q+2 \\ \vdots & \vdots & \vdots & & \vdots \\ q & 2q & 3q & \cdots & pq \end{array}$$

If $gcd(k,q) = d > 1$ then no element in the row which has k as the first element is relatively prime to pq. For if $gcd(tq+k, pq) = 1$ for some $1 \leq t < p$ then there exist integers α and β such that $\alpha(tq+k) + \beta pq = 1$. But then $d|(\alpha(tq+k)+\beta pq) = 1$, i.e. $d = 1$ a contradiction. Hence, all numbers which are relatively prime to pq must lie in a row whose first element is relatively prime to q. Since there are $\phi(q)$ such rows, our proof will be complete if we can show that there are $\phi(p)$ elements in each such row which are relatively prime to pq.
Consider the k-th row:

$$k \quad q+k \quad 2q+k \quad \cdots \quad (p-1)q+k,$$

where $gcd(k,q) = 1$. Suppose $iq + k \equiv jq + k (mod\ p)$, with $0 \leq i, j < p$. Then p divides $iq + k - (jq + k) = (i - j)q$. But, since $gcd(p,q) = 1$, it follows from Lemma 13.1 that p divides $i - j$. But $|i - j| < p$ so that we must have $i = j$. Therefore, no two elements in the k-th row are congruent $(\mathrm{mod}\, p)$. Now, if $tq+k$ is any element of the k-th row then one can easily show that $gcd(tq + k, q) = gcd(k, q) = 1$. Since no two elements are congruent, their remainders of the division by p are $0, 1, 2, \cdots, p-1$, in some order. By definition, exactly $\phi(p)$ elements of $\{0, 1, ..., p-1\}$ are relatively prime to p. But if $gcd(tq+k, p) = 1$ then $gcd(tq+k, pq) = 1$ since $gcd(tq+k, q) = 1$ (See proof of Theorem 13.4. It follows that there are exactly $\phi(p)$ elements in the k-th row which are relatively prime to pq which completes the proof.■

Corollary 13.2
If p and q are primes then $\phi(pq) = (p-1)(q-1)$.

Proof.
By Theorem 13.6 we have $\phi(pq) = \phi(p)\phi(q)$ since $gcd(p,q) = 1$. By Theorem 13.5, we have $\phi(p) = p - 1$ and $\phi(q) = q - 1$. Hence, $\phi(pq) = \phi(p)\phi(q)$.■

Corollary 13.3
If $n = p_1^{e_1} p_2^{e_2} \cdots p_k^{e_k}$ then

$$\phi(n) = (p_1^{e_1} - p_1^{e_1-1})(p_2^{e_2} - p_2^{e_2-1}) \cdots (p_k^{e_k} - p_k^{e_k-1}).$$

Proof.
Applying the multiplicative property repeatedly we have

$$\begin{aligned}
\phi(n) &= \phi(p_1^{e_1})\phi(p_2^{e_2}\cdots p_k^{e_k}) \quad since\ gcd(p_1^{e_1}, p_2^{e_2}\cdots p_k^{e_k}) = 1 \\
&= \phi(p_1^{e_1})\phi(p_2^{e_2})\phi(p_3^{e_3}\cdots p_k^{e_k}) \quad since\ gcd(p_2^{e_2}, p_3^{e_3}\cdots p_k^{e_k}) = 1 \\
&\vdots \\
&= \phi(p_1^{e_1})\phi(p_2^{e_2})\cdots\phi(p_k^{e_k}) \\
&= (p_1^{e_1} - p_1^{e_1-1})(p_2^{e_2} - p_2^{e_2-1})\cdots(p_k^{e_k} - p_k^{e_k-1}) \quad by\ Theorem\ 13.5
\end{aligned}$$

■