The least positive common multiple is said to be the least common multiple (l.c.m) of the integers $a_1, a_2 \cdots a_n$. For example, the l.c.m of 2, 3, 6 is 6; the l.c.m $-2, -3, -6$ is 6; the l.c.m of $-2, -6, 10$ is 30

Worked Examples 1. Solve the system of linear congruence

$$x \equiv 1 \pmod 3, \quad x \equiv 2 \pmod 5, \quad x \equiv 3 \pmod 7$$

Solution: 3, 5 and 7 are pairwise prime to each other.

Let $m = 3.5.7 = 105$.

Let $M_1 = \frac{m}{3} = 35$, $M_2 = \frac{m}{5} = 21$, $M_3 = \frac{m}{7} = 15$

Then $\gcd(M_1, 3) = 1$, $\gcd(M_2, 5) = 1$, $\gcd(M_3, 7) = 1$

$\gcd(35, 3) = 1$. Therefore the linear congruence $35x \equiv 1 \pmod 3$ has a unique solution and the solution is $x \equiv 2 \pmod 3$

$\gcd(21, 5) = 1$. Therefore the linear congruence $21x \equiv 1 \pmod 5$ has a unique solution and the solution is $x \equiv 1 \pmod 5$.

$\gcd(15, 7) = 1$. Therefore the linear congruence $15x \equiv 1 \pmod 7$ has a unique solution and the solution is $x \equiv 1 \pmod 7$.

$x_0 = 1.(35.2) + 2(21.1) + 3.(15.1) = 157$ is a solution of the system of linear congruence by Chinese Remainder Theorem.

So, the solution of the given system is $x \equiv 157 \pmod{105}$, which is equivalent $x \equiv 52 \pmod{105}$

2. Find four consecutive integers divisible by 3, 4, 5, 7 respectively.

Solution: Let $n, n+1, n+2, n+3$ be four consecutive integers divisible by 3, 4, 5, 7 respectively.

Then $n \equiv 0 \pmod 3$, $n+1 \equiv 0 \pmod 4$, $n+2 \equiv 0 \pmod 5$, $n+3 \equiv 0 \pmod 7$.

We are to solve simultaneous linear congruences $n \equiv 0 \pmod 3$, $n \equiv 3 \pmod 4$, $n \equiv 3 \pmod 5$, $n \equiv 4 \pmod 7$

3, 4, 5, 7 are pairwise prime to each other. Let $m = 3.4.5.7 = 420$

Let $M_1 = \frac{m}{3} = 140$, $M_2 = \frac{m}{4} = 105$, $M_3 = \frac{m}{5} = 84$ and

$M_4 = \frac{m}{7} = 60$

Since $\gcd(M_1, 3) = \gcd(140, 3) = 1$, the linear congruence $140x \equiv 1 \pmod 3$ has a unique solution (mod 3) and the solution is $x = 2$

Since $\gcd(M_2, 4) = \gcd(105, 4) = 1$, the linear congruence $105x \equiv 1 \pmod 4$ has a unique solution (mod 4) and the solution is $x = 1$

Since $\gcd(M_3, 5) = \gcd(84, 5) = 1$, the linear congruence $84x \equiv 1 \pmod 5$ has unique solution (mod 5) and the solution is $x = 4$

Since $\gcd(M_4, 7) = \gcd(60, 7) = 1$, the linear congruence $60x \equiv 1 \pmod 7$ has unique solution (mod 7) and the

solution is $x = 2$. Therefore by Chinese Remainder Theorem

$x_0 = 0.140.2 + 3.105.1 + 3.84.4 + 4.60.2 = 315 + 1008 + 480 = 1803$

is a solution of the system of linear congruences and

the solution is unique modulo 420

$\therefore x_0 \equiv 123 \pmod{420}$. Therefore the consecutive integers

are $n, n+1, n+2, n+3$, when $n = 123 + 420t$, $t = 0, \pm 1, \pm 2, \cdots$

Theorem 2.5.8 (Fundamental theorem of Arithmetic)

Any positive integer is either 1, or a prime, or it can be expressed as a product of primes, the representation being unique except for the order of the prime factors.

Proof: Let n be a positive integer. Either $n = 1$ or $n > 1$.

Let $P(n)$ be the statement that $n\ (>1)$ is either a prime or it can be expressed as a product of primes.

$P(2)$ is true, since 2 is prime.

Let us assume that $P(n)$ is true for all n, where n is a positive integer such that $2 \le n \le k$

If $k+1$ be itself a prime then $P(k+1)$ is true and by the second principle of induction, $P(n)$ is true for all positive integer $n > 1$.

If $k+1$ be not a prime then it is a composite number.

Let $k+1 = rs$ where r, s are integers with $2 \leq r < k+1$, $2 \leq s < k+1$.

By induction hypothesis, $P(r)$ and $P(s)$ are both true.

Then $r = p_1 p_2 \cdots p_i$, where $p_1, p_2, \cdots, p_i$ are primes, $i \geq 1$;

$s = q_1 q_2 \cdots q_j$, where $q_1, q_2, \cdots, q_j$ are primes, $j \geq 1$.

Thus $k+1$ is expressed as the product of primes and $P(k+1)$ is proved to be true. By the second principle of induction $P(n)$ is true for all positive integers $n > 1$.

Hence the first part of the theorem is established

In order to prove the uniqueness of the representation, let us assume that $n = p_1 p_2 \cdots p_k = q_1 q_2 \cdots q_m$ where $p_1, p_2, \cdots, p_k$ and $q_1, q_2, \cdots, q_m$ are all primes.

Since $p_1 \mid n$, it follows that $p_1 \mid q_1 q_2 \cdots q_m$.

Since p_1 is a prime, $p_1 \mid q_r$ for some r where $1 \leq r \leq m$.

But since p_1 and q_r are both primes, $p_1 = q_r$.

We obtain $p_2 p_3 \cdots p_k = q_1 q_2 \cdots q_{r-1} q_{r+1} \cdots q_m$.

We repeat the argument with p_2 and obtain $p_2 = q_s$ for some s, $1 \leq s \leq m$, $s \neq r$. Then

$$p_3 p_4 \cdots p_k = q_1 q_2 \cdots q_{r-1} q_{r+1} \cdots q_{s-1} q_{s+1} \cdots q_m$$