# Chapter 2: The Integers' Solutions

Saif Mohammed

October 18, 2024

**Exercise 3.** Prove that the set of all linear combinations of $a$ and $b$ are precisely the multiples of $\gcd(a, b)$.

*Solution.* Let $d = \gcd(a, b)$ and $c = ax + by$ for $c, x, y \in \mathbb{Z}$. We prove $c$ is a multiple of $d$.

Let $a = da'$ and $b = db'$. So $c = ax + by = d(a'x + b'y)$. Hence, $d \mid c$.

We now prove the converse: if $c$ is a multiple of $d$, then it is a linear combination of $a$ and $b$.

Let $c = dc'$. We know $d$ is the least positive linear combination of $a$ and $b$. So

$$\begin{aligned} & d = am + bn && [\text{for } m, n \in \mathbb{Z}] \\ \implies & dc' = amc' + bnc' \\ \implies & c = a(mc') + b(nc'). \end{aligned}$$

Hence, we proved $c$ is a linear combination of $a$ and $b$. □

**Exercise 4.** Two numbers are said to be relatively prime if their gcd is 1. Prove that $a$ and $b$ are relatively prime if and only if every integer can be written as a linear combination of $a$ and $b$.

*Solution.* Suppose $a$ and $b$ are relatively prime. We know that $ax + by = \gcd(a, b) = 1$ for some $x, y \in \mathbb{Z}$. As every integer is a multiple of 1, then by **(3)**, every integer can be written as a linear combination of $a$ and $b$.

Now, we prove the the converse: if every integer can be written as a linear combination of $a$ and $b$, then $\gcd(a, b) = 1$.

As 1 is the least positive integer and we know that $\gcd(a, b)$ must be the least positive linear combination, we can conclude that $\gcd(a, b) = 1$. □

**Exercise 5.** Prove Theorem 2.6. That is, use induction to prove that if the prime $p$ divides $a_1 a_2 \cdots a_n$, then $p$ divides $a_i$, for some $i$.

*Solution.* If $p \mid a_1$, then the statement is trivially true. Now suppose if $p \mid a_1 a_2 \cdots a_k$, then $p \mid a_i$ for some $i$. Now for $p \mid a_1 a_2 \cdots a_{k+1}$, if we bring out a $a_{k+1}$, then there can happen two cases.

**Case 1:** $p \mid a_{k+1}$. If so, then the statement is obviously true.

**Case 2:** $p \nmid a_{k+1}$. Is so, then we can say $p \mid a_1 a_2 \cdots a_k$. And by the induction hypothesis, there is$a_i$ for some $i$ such that $p \mid a_i$.

Hence, the theorem is proved.

[Note: In each case, any $a_n$ not necessarily the same with other $a_n$'s. So, $a_1$ of the base case, $a_1, a_2, \ldots, a_k$ of the induction hypothesis, and $a_1, a_2, \ldots, a_k$ of the inductive step are not necessarily are the same numbers.] □

**Exercise 7.** (a) A natural number greater than 1 that is not prime is called **composite**. Show that for any $n$, there is a run of $n$ consecutive composite numbers. *Hint:* Think factorial.

(b) Therefore, there is a string of 5 consecutive composite numbers starting where?

*Solution.* Left for later. □

**Exercise 9.** Notice that $\gcd(30, 50) = 5 \gcd(6, 10) = 5 \cdot 2$. In fact, this is always true; prove that if $a \neq 0$, then $\gcd(ab, ac) = a \cdot \gcd(b, c)$.

*Solution.* $\gcd(ab, ac) = abx + acy = a(bx + cy)$ for some $x, y \in \mathbb{Z}$. Now $\gcd(b, c)$ is multiple of any linear combination of $b$ and $c$, so

$$\gcd(b, c) \mid bx + cy \implies a \cdot \gcd(b, c) \mid a(bx + cy) \implies a \cdot \gcd(b, c) \mid \gcd(ab, ac).$$

Again, for some $x', y' \in \mathbb{Z}$ $\gcd(b, c) = bx' + cy' \implies a \cdot \gcd(b, c) \implies abx' + acy'$. As $\gcd(ab, ac)$ is multiple of any linear combination of $ab$ and $ac$, so

$$\gcd(ab, ac) \mid abx' + acy' \implies \gcd(ab, bc) \mid a \cdot \gcd(b, c)$$

Because $a \cdot \gcd(b, c) \mid \gcd(ab, ac)$ and $\gcd(ab, bc) \mid a \cdot \gcd(b, c)$, it can be concluded that $\gcd(ab, ac) = a \cdot \gcd(b, c)$. □

**Exercise 10.** Suppose that two integers $a$ and $b$ have been factored into primes as follows:

$$a = p_1^{n_1} p_2^{n_2} \cdots p_r^{n_r}$$

and

$$b = p_1^{m_1} p_2^{m_2} \cdots p_r^{m_r},$$

where the $p_i$'s are primes, and the exponents $m_i$ and $n_i$ are non-negative integers. It is the case that

$$\gcd(a, b) = p_1^{s_1} p_2^{s_2} \cdots p_r^{s_r},$$

where $s_i$ is the smaller of $n_i$ and $m_i$. Show this with $a = 360 = 2^3 3^2 5^1$ and $b = 900 = 2^2 3^2 5^2$. Now prove this fact in general.

*Solution.* For $r = 1$, $a = p_1^{n_1}$ and $b = p_1^{m_1}$, where WLOG, $n_1 > m_1 = s_1$. We can rewrite $a = p_1^{s_1} p_1^{n_1 - s_1}$ and so $\gcd(a, b) = p_1^{s_1} \cdot \gcd(p_1^{n_1 - s_1}, 1) = p_1^{s_1}$.

Let up to $r = k$ this holds. Now for $r = k + 1$, there are two cases. WLOG, $n_{k+1} > m_{k+1} = s_{k+1}$.

$$\begin{aligned}
\gcd(a, b) &= p_{k+1}^{s_{k+1}} \cdot \gcd(p_1^{n_1} p_2^{n_2} \cdots p_k^{n_k}, p_1^{m_1} p_2^{m_2} \cdots p_k^{m_k} p_{k+1}^{m_{k+1} - s_{k+1}}) \\
&= p_{k+1}^{s_{k+1}} \cdot \gcd(p_1^{n_1} p_2^{n_2} \cdots p_k^{n_k}, p_1^{m_1} p_2^{m_2} \cdots p_k^{m_k}) && \text{[no common divisor exists between a prime and other primes.]} \\
&= p_1^{s_1} p_2^{s_2} \cdots p_k^{s_k} p_{k+1}^{s_{k+1}} && \text{[by induction hypothesis.]}
\end{aligned}$$

□

**Exercise 11.** The least common multiple of natural numbers $a$ and $b$ is the smallest positive common multiple of $a$ and $b$. That is, if $m$ is the least common multiple of $a$ and $b$, then $a \mid m$ and $b \mid m$, and if $a \mid n$ and $b \mid n$ then $n \geq m$. We will write $\operatorname{lcm}(a, b)$ for the least common multiple of $a$ and $b$. Find $\operatorname{lcm}(20, 114)$ and $\operatorname{lcm}(14, 45)$. Can you find a formula for the lcm of the type given for the gcd in the previous exercise?

*Solution.* If $a = p_1^{n_1} p_2^{n_2} \cdots p_r^{n_r}$ and $b = p_1^{m_1} p_2^{m_2} \cdots p_r^{m_r}$, then we claim that

$$\operatorname{lcm}(a, b) = p_1^{l_1} p_2^{l_2} \cdots p_r^{l_r}$$

where $l_i$ is the largest of $n_i$ and $m_i$.

Now we prove that. Let $c = p_1^{l_1} p_2^{l_2} \cdots p_r^{l_r}$. As $l_i$ is the largest of $n_i$ and $m_i$, it is always larger than or equal to the corresponding power of factorization of either $a$ or $b$. So $a \mid c$ and $b \mid c$.

Now let's take another common multiple of $a$ and $b$, $d = p_1^{w_1} p_2^{w_2} \cdots p_r^{w_r}$. So

$$a \mid d \implies p_i^{n_i} \mid p_i^{w_i} \implies n_i \mid w_i \implies n_i \leq w_i$$

and

$$b \mid d \implies p_i^{m_i} \mid p_i^{w_i} \implies m_i \mid w_i \implies m_i \leq w_i$$

It follows that $w_i$ is larger than or equal to the the largest of $n_i$ and $m_i$. That is, $w_i \geq l_i$. Hence, $c \mid d \implies c \leq d$. Thus, we can conclude $c$ is indeed the lcm of $a$ and $b$. □

**Exercise 12.** Show that if $\gcd(a, b) = 1$, then $\operatorname{lcm}(a, b) = ab$. In general, show that

$$\operatorname{lcm}(a, b) = \frac{ab}{\gcd(a, b)}.$$

*Solution.* For $a = p_1^{n_1} p_2^{n_2} \cdots p_r^{n_r}$ and $b = p_1^{m_1} p_2^{m_2} \cdots p_r^{m_r}$, we know,

$$\text{lcm}(a,b) = p_1^{l_1} p_2^{l_2} \cdots p_r^{l_r} \qquad [l_i \text{ is the largest of } m_i \text{ and } n_i.] \tag{1}$$

$$\text{and} \quad \gcd(a,b) = p_1^{s_1} p_2^{s_2} \cdots p_r^{s_r} \qquad [s_i \text{ is smallest of } m_i \text{ and } n_i.] \tag{2}$$

Let $m_i \geq n_i$ for some $i \in \mathbb{N}$. So $l_i = m_i$ and $s_i = n_i$. Hence, $p_i^{l_i} \cdot p_i^{s_i} = p_i^{m_i} \cdot p_i^{n_i}$. Similarly, we can show that for $m_i \leq n_i$, $p_i^{l_i} \cdot p_i^{s_i} = p_i^{m_i} \cdot p_i^{n_i}$. It follows that if we multiply (1) and (2), then $p_i^{m_i}$ and $p_i^{n_i}$ both exists for any $i \in \mathbb{N}$ as factors of the product. By rearranging them, we can write

$$\begin{aligned} \text{lcm}(a,b) \cdot \gcd(a,b) &= p_1^{n_1} p_2^{n_2} \cdots p_r^{n_r} \cdot p_1^{m_1} p_2^{m_2} \cdots p_r^{m_r} \\ \implies \text{lcm}(a,b) \cdot \gcd(a,b) &= ab \\ \implies \text{lcm}(a,b) &= \frac{ab}{\gcd(a,b)}. \end{aligned}$$

□

**Exercise 13.** Prove that if $m$ is a common multiple of both $a$ and $b$, then $\text{lcm}(a,b) \mid m$.

*Solution.* Let $l = \text{lcm}(a,b)$. Let's assume that $l \nmid m$. So, $m = l \cdot k + r$, where $k \in \mathbb{N}$ and $0 < r <\mid l \mid$. Here, $a \mid m$ and $b \mid m$ and also $a \mid l$ and $b \mid l$, so $a \mid r$ and $b \mid r$.

So we see that $r$ is a common multiple of $a$ and $b$, which is less than $l$, but this is not possible because $l$ is the least common multiple of $a$ and $b$. Therefore, $l \mid m \implies \text{lcm}(a,b) \mid m$. □