ANSWER on Question #80976 – Math – Combinatorics | Number Theory

QUESTION

1. **Theorem**. Let a,b and c be integers with a and b not both 0. If $x = x_0$, $y = y_0$ is an integer solution to the equation $ax + by = c$ that is, $ax_0 + by_0 = c$, then for every integer k, the numbers $x = x_0 + kb\ (a,b)$ and $y = y_0 - ka\ (a,b)$ are integers that also satisfy the linear Diophantine equation $ax + by = c$. Moreover, every solution to the linear Diophantine equation $ax + by = c$ is of this form.

2. Exercise Find all integer solutions to the equation $24x + 9y = 33$.

3. **Theorem**. Let a and b be integers with $a, b > 0$. Then $\gcd(a,b) \cdot lcm(a,b) = ab$.

SOLUTION

1. Let we know that $x = x_0$, $y = y_0$ is an integer solution to the equation $ax + by = c$. Then,

$$ax_0 + by_0 = c$$

Consider the system of equations

$$\begin{cases} ax_0 + by_0 = c \\ ax + by = c \end{cases} \to ax_0 + by_0 = ax + by \to ax_0 - ax = by - by_0 \to$$

$$a \cdot (x_0 - x) = b \cdot (y - y_0) | \div (ab) \to \boxed{\underbrace{\frac{x_0 - x}{b}}_{f(x)} = \underbrace{\frac{y - y_0}{a}}_{g(y)}}$$

We have obtained an equation where the function $f(x)$ on the left-hand side and $g(y)$ on the right-hand side. These are functions of various independent variables x, y. Since this equation must be satisfied for all values of x, y, these functions can only be constants $-k$. Then,

$$\frac{x_0 - x}{b} = -k = \frac{y - y_0}{a} \to \begin{cases} x_0 - x = -kb \\ y - y_0 = -ka \end{cases} \to \boxed{\begin{cases} x = x_0 + kb \\ y = y_0 - ka \end{cases}}$$

Q.E.D.

2.

$$24x + 9y = 33$$

1 STEP: Let us find a particular solution of the given Diophantine equation.

Let us check that a pair of numbers $x_0 = 1$ and $y_0 = 1$ is a solution of the given equation:

$$24 \cdot 1 + 9 \cdot 1 = 3$$

2 STEP: We use the result of the theorem from part (1)

$$\begin{cases} 24x + 9y = 3 \\ x_0 = 1 \\ y_0 = 1 \end{cases} \rightarrow \boxed{\begin{cases} x = 1 + 9k \\ y = 1 - 24k \\ k \in \mathbb{Z} \end{cases}}$$

3.

First we prove an auxiliary lemma.

<u>Lemma</u>: If $m > 0$, $lcm(ma, mb) = m \cdot lcm\,(a, b)$.

Since $lcm(ma, mb)$ is a multiple of ma, which is a multiple of m, we have $m|lcm\,(ma, mb)$.

Let $mh_1 = lcm(ma, mb)$, and set $h_2 = lcm(a, b)$. Then $ma|mh_1 \Rightarrow a|h_1$ and $mb|mh_1 \Rightarrow b|h_1$. That says h_1 is a common multiple of a and b; but h_2 is the least common multiple, so $h_1 \geq h_2$.

Next, $a|h_2 \Rightarrow am|mh_2$ and $b|h_2 \Rightarrow bm|mh_2$. Since mh_2 is a common multiple of ma and mb, and

$mh_1 = lcm(ma, mb)$, we have $mh_2 \geq mh_1$, i.e. $h_2 \geq h_1$.

Then,

$$\begin{cases} h_1 \geq h_2 \\ h_2 \geq h_1 \end{cases} \rightarrow h_1 = h_2$$

Therefore, $lcm(ma, mb) = mh_1 = mh_2 = m \cdot lcm(a, b)$; proving the Lemma.

Conclusion of Proof of Theorem: Let $g = gcd(a, b)$. Since $g|a$, $g|b$, let $a = gc$ and $b = gd$.

From a result in the text,

$$gcd(c, d) = gcd\left(\frac{a}{g}, \frac{b}{g}\right) = 1$$

Now we will prove that $lcm(c, d) = cd$. Since $c|lcm(c, d)$, let $lcm(c, d) = kc$. Since $d|kc$ and $gcd(c, d) = 1$, $d|k$ and so $dc \le kc$. However, kc is the least common multiple and dc is a common multiple, so $kc \le dc$. Hence $kc = dc$, i.e. $lcm(c, d) = cd$. Finally, using the Lemma and $lcm(c, d) = cd$, we have:

$$lcm(a, b) \cdot \mathrm{gcd}(a, b) = lcm(gc, gd) \cdot g = g \cdot lcm(c, d) \cdot g = gcdg = (gc)(gd) = ab$$

Q.E.D.