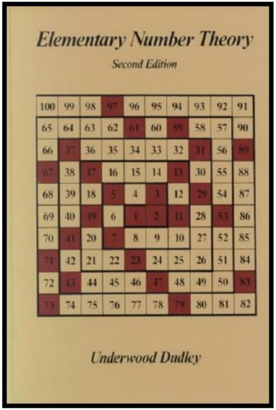
Elementary Number Theory

Section 3. Linear Diophantine Equations—Proofs of Theorems



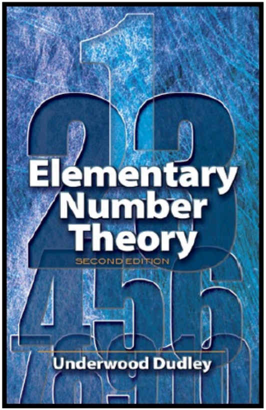


Table of contents

Lemma 3.1

Lemma 3.1. If $x = x_0$ and $y = y_0$ is a solution of $ax + by = c$, then so is $x = x_0 + bt$ and $y = y_0 - at$ for any integer $t \in \mathbb{Z}$.

Proof. Since $x = x_0$ and $y = y_0$ is a solution, then $ax_0 + by_0 = c$. We simply substitute $x = x_0 + bt$ and $y = y_0 - at$ and confirm that it is a solution. We have

$$a(x_0 + bt) + b(y_0 - at) = ax_0 + abt + by_0 - bat = ax_0 + by_0 = c,$$

as claimed. □

Lemma 3.1

Lemma 3.1. If $x = x_0$ and $y = y_0$ is a solution of $ax + by = c$, then so is $x = x_0 + bt$ and $y = y_0 - at$ for any integer $t \in \mathbb{Z}$.

Proof. Since $x = x_0$ and $y = y_0$ is a solution, then $ax_0 + by_0 = c$. We simply substitute $x = x_0 + bt$ and $y = y_0 - at$ and confirm that it is a solution. We have

$$a(x_0 + bt) + b(y_0 - at) = ax_0 + abt + by_0 - bat = ax_0 + by_0 = c,$$

as claimed. □

Lemma 3.2

Lemma 3.2. If $(a, b) \not| c$ then $ax + by = c$ has no solutions, and if $(a, b) \mid c$ then $ax + by = c$ has a solution.

Proof. Suppose there is a solution to $ax + by = c$, say $x = x_0$, $y = y_0$. Then $ax_0 + by_0 = c$. Also $(a, b) \mid ax_0$ and $(a, b) \mid by_0$. So by Lemma 1.1, we have $(a, b) \mid c$. That is, if $ax + by = c$ has a solution then $(a, b) \mid c$. The (logically equivalent) contrapositive of this implication is: "If $(a, b) \mid c$ then $ax + by = c$ does not have a solution." So the first claim holds.

Lemma 3.2

Lemma 3.2. If $(a, b) \not| c$ then $ax + by = c$ has no solutions, and if $(a, b) \mid c$ then $ax + by = c$ has a solution.

Proof. Suppose there is a solution to $ax + by = c$, say $x = x_0$, $y = y_0$. Then $ax_0 + by_0 = c$. Also $(a, b) | ax_0$ and $(a, b) \mid by_0$. So by Lemma 1.1, we have $(a, b) \mid c$. That is, if $ax + by = c$ has a solution then $(a, b) \mid c$. The (logically equivalent) contrapositive of this implication is: "If $(a, b) \mid c$ then $ax + by = c$ does not have a solution." So the first claim holds.

Now suppose that $(a, b) \mid c$. Then $c = m(a, b)$ for some integer m. By Theorem 1.4, there are integers r and s such that $ar + bs = (a, b)$. Then $m(ar + bs) = m(a, b)$ or $a(rm) + b(sm) = m(a, b) = c$, so we have $x = rm$, $y = sm$ as a solution to $ax + by = c$. That is, the second claim holds. □

Lemma 3.2

Lemma 3.2. If $(a, b) \nmid c$ then $ax + by = c$ has no solutions, and if $(a, b) \mid c$ then $ax + by = c$ has a solution.

Proof. Suppose there is a solution to $ax + by = c$, say $x = x_0$, $y = y_0$. Then $ax_0 + by_0 = c$. Also $(a, b) \mid ax_0$ and $(a, b) \mid by_0$. So by Lemma 1.1, we have $(a, b) \mid c$. That is, if $ax + by = c$ has a solution then $(a, b) \mid c$. The (logically equivalent) contrapositive of this implication is: "If $(a, b) \mid c$ then $ax + by = c$ does not have a solution." So the first claim holds.

Now suppose that $(a, b) \mid c$. Then $c = m(a, b)$ for some integer m. By Theorem 1.4, there are integers r and s such that $ar + bs = (a, b)$. Then $m(ar + bs) = m(a, b)$ or $a(rm) + b(sm) = m(a, b) = c$, so we have $x = rm$, $y = sm$ as a solution to $ax + by = c$. That is, the second claim holds. $\square$

Exercise 3.3(b).

Exercise 3.3(b). Find all solutions of $14x + 35y = 91$.

Solution. First, we find the greatest common divisor of the coefficients: $(a, b) = (14, 35) = 7 = d$. Notice that $7 \mid 91$ (or $(a, b) \mid c$) so that by Lemma 3.2 the given equation has a solution. Dividing the both sides of $14x + 35y = 91$ by 7, gives $2x + 5y = 13$ (or $a'x + b'y = c'$ where $a' = 2$, $b' = 5$, and $c' = 13$).

Exercise 3.3(b).

Exercise 3.3(b). Find all solutions of $14x + 35y = 91$.

Solution. First, we find the greatest common divisor of the coefficients: $(a, b) = (14, 35) = 7 = d$. Notice that $7 \mid 91$ (or $(a, b) \mid c$) so that by Lemma 3.2 the given equation has a solution. Dividing the both sides of $14x + 35y = 91$ by 7, gives $2x + 5y = 13$ (or $a'x + b'y = c'$ where $a' = 2$, $b' = 5$, and $c' = 13$). Now if we can find one solution of $2x + 5y = 13$, then we can find infinitely many solutions using Lemma 3.1 (and we will see that the solutions given by Lemma 3.1 are *all* of the solutions in Lemma 3.3). Observe that $x_0 = 4$ and $y_0 = 1$ is a solution. By Lemma 3.1, $x = x_0 + b't = 4 + 5t$ and $y = y_0 - a't = 1 - 2t$ is a solution for all $t \in \mathbb{Z}$. By Lemma 3.3 (to be done next), these are all of the solutions of the original equation: $\boxed{x = 4 + 5t \text{ and } y = 1 - 2t \text{ for } t \in \mathbb{Z}.}$ $\square$

Exercise 3.3(b).

Exercise 3.3(b). Find all solutions of $14x + 35y = 91$.

Solution. First, we find the greatest common divisor of the coefficients: $(a, b) = (14, 35) = 7 = d$. Notice that $7 \mid 91$ (or $(a, b) \mid c$) so that by Lemma 3.2 the given equation has a solution. Dividing the both sides of $14x + 35y = 91$ by 7, gives $2x + 5y = 13$ (or $a'x + b'y = c'$ where $a' = 2$, $b' = 5$, and $c' = 13$). Now if we can find one solution of $2x + 5y = 13$, then we can find infinitely many solutions using Lemma 3.1 (and we will see that the solutions given by Lemma 3.1 are *all* of the solutions in Lemma 3.3). Observe that $x_0 = 4$ and $y_0 = 1$ is a solution. By Lemma 3.1, $x = x_0 + b't = 4 + 5t$ and $y = y_0 - a't = 1 - 2t$ is a solution for all $t \in \mathbb{Z}$. By Lemma 3.3 (to be done next), these are all of the solutions of the original equation: $\boxed{x = 4 + 5t \text{ and } y = 1 - 2t \text{ for } t \in \mathbb{Z}.}$ $\square$

Lemma 3.3

Lemma 3.3. Suppose that $(a, b) = 1$ and $x = x_0$, $y = y_0$ is a solution of $ax + by = c$. Then all solutions of $ax + by = c$ are given by $x = x_0 + bt$, $y = y_0 - at$ where $t \in \mathbb{Z}$.

Proof. Since we have hypothesized that $(a, b) = 1$ then we have $(a, b) \mid c$ and by Lemma 3.2 we know that the equation has a solution. Let $x = r$, $y = s$ be any solution; we want to show that $r = x_0 + bt$, $y = y_0 - at$ for some integer t. Since $x = x_0$, $y = y_0$ is a solution, then we have $ax_0 + by_0 = c$ and hence

$$c - c = (ax_0 + by_0) - (ar + bs) \text{ or } a(x_0 - r) + b(y_0 - s) = 0. \quad (*)$$

Lemma 3.3

Lemma 3.3. Suppose that $(a, b) = 1$ and $x = x_0$, $y = y_0$ is a solution of $ax + by = c$. Then all solutions of $ax + by = c$ are given by $x = x_0 + bt$, $y = y_0 - at$ where $t \in \mathbb{Z}$.

Proof. Since we have hypothesized that $(a, b) = 1$ then we have $(a, b) \mid c$ and by Lemma 3.2 we know that the equation has a solution. Let $x = r$, $y = s$ be any solution; we want to show that $r = x_0 + bt$, $y = y_0 - at$ for some integer t. Since $x = x_0$, $y = y_0$ is a solution, then we have $ax_0 + by_0 = c$ and hence

$$c - c = (ax_0 + by_0) - (ar + bs) \text{ or } a(x_0 - r) + b(y_0 - s) = 0. \quad (*)$$

Since $a \mid a(x_0 - r)$ and $a \mid 0$ then by Lemma 1.2 $a \mid b(y_0 - s)$. Since $(a, b) = 1$ by hypothesis, then by Corollary 1.1 we have that $a \mid (y_0 - s)$. That is (by the definition of divisibility), $at = y_0 - s$ for some integer t, or $s = y_0 - at$ where $t \in \mathbb{Z}$, as claimed.

Lemma 3.3

Lemma 3.3. Suppose that $(a, b) = 1$ and $x = x_0$, $y = y_0$ is a solution of $ax + by = c$. Then all solutions of $ax + by = c$ are given by $x = x_0 + bt$, $y = y_0 - at$ where $t \in \mathbb{Z}$.

Proof. Since we have hypothesized that $(a, b) = 1$ then we have $(a, b) \mid c$ and by Lemma 3.2 we know that the equation has a solution. Let $x = r$, $y = s$ be any solution; we want to show that $r = x_0 + bt$, $y = y_0 - at$ for some integer t. Since $x = x_0$, $y = y_0$ is a solution, then we have $ax_0 + by_0 = c$ and hence

$$c - c = (ax_0 + by_0) - (ar + bs) \text{ or } a(x_0 - r) + b(y_0 - s) = 0. \quad (*)$$

Since $a \mid a(x_0 - r)$ and $a \mid 0$ then by Lemma 1.2 $a \mid b(y_0 - s)$. Since $(a, b) = 1$ by hypothesis, then by Corollary 1.1 we have that $a \mid (y_0 - s)$. That is (by the definition of divisibility), $at = y_0 - s$ for some integer t, or $s = y_0 - at$ where $t \in \mathbb{Z}$, as claimed.

Lemma 3.3 (continued)

Lemma 3.3. Suppose that $(a, b) = 1$ and $x = x_0$, $y = y_0$ is a solution of $ax + by = c$. Then all solutions of $ax + by = c$ are given by $x = x_0 + bt$, $y = y_0 - at$ where $t \in \mathbb{Z}$.

Proof (continued). Since $a(x_0 - r) + b(y_0 - s) = 0$ by $(*)$, then $a(x_0 - r) + b(at) = 0$ or $(x_0 - r) + bt = 0$ (since $a \neq 0$, as implied by the hypothesis that $(a, b) = 1$). That is, $r = x_0 + bt$ where $t \in \mathbb{Z}$, as claimed. Since $x = r$ and $y = s$ is an arbitrary solution, then the result follows. $\square$