Example 20. (review)

- $56x + 72y = 15$ has no integer solutions (because the left side is even but the right side is odd).
- $56x + 72y = 2$ has no integer solutions (because $8|(56x + 72y)$ but $8\nmid 2$).
- $56x + 72y = 8$ has an integer solution (that's Bezout's identity!) and we can find it using the Euclidean algorithm ($\gcd(56, 72) = 8$).

  [To make our life easier, we divide by 8 to get the equivalent equation $7x + 9y = 1$. One solution is $(x, y) = (4, -3)$.]
- $56x + 72y = k$ has an integer solution if and only if k is a multiple of $\gcd(56, 72) = 8$.

Example 21. Find the general solution to the diophantine equation $56x + 72y = 24$.

Solution. We first note that this equation has an integer solution because 24 is a multiple of $\gcd(56, 72) = 8$.

To make our life easier, we divide by 8 to get the equivalent equation $7x + 9y = 3$.

As observed above, a solution to $7x + 9y = 1$ is $(x, y) = (4, -3)$ (and we can always find such a solution using the Euclidean algorithm). Therefore, a solution to $7x + 9y = 3$ is $(x, y) = 3\cdot(4, -3) = (12, -9)$.

To get the general solution, we need to add the solutions to the homogeneous equation $56x + 72y = 0$. First, it is important to cancel common factors and write this as $7x + 9y = 0$. In that form, we can see that the solutions are $(x, y) = (9t, -7t)$ where t is any integer.

Note. We're not missing any solutions by restricting t to integers because $\gcd(9, 7) = 1$. We would be missing solutions by only considering $(x, y) = (72t, -56t)$ where t is an integer (for instance, $t = 1/2$ produces an integer solution).

In conclusion, the general solution to the diophantine equation $56x + 72y = 24$ is $(x, y) = (12 + 9t, -9 - 7t)$, that is, $x = 12 + 9t$ and $y = -9 - 7t$, where t is any integer.

Note that we can focus on diophantine equations $ax + by = c$ with $\gcd(a, b) = 1$.

(Just divide both sides by $\gcd(a, b)$.)

Theorem 22. The diophantine equation $ax + by = c$ with $\gcd(a, b) = 1$ has the general solution

$$x = x_0 + bt, \quad y = y_0 - at,$$

where $t\in\mathbb{Z}$ is a parameter, and x_0, y_0 is any particular solution.

How to find a particular solution? Since $\gcd(a, b) = 1$, we can find integers x_1, y_1 such that $ax_1 + by_1 = 1$ (this is Bezout's identity). Multiply both sides with c, to see that we can take $x_0 = cx_1$ and $y_0 = cy_1$.

Proof. First, let us consider the case of any real solutions. The general solution of $ax + by = c$ (which describes a line!) can be described as

$$x = x_0 + bt, \quad y = y_0 - at.$$

Since $\gcd(a, b) = 1$, this solution will be integers if and only if t is an integer. □

Example 23. (extra) Determine all solutions to the diophantine equation $56x + 72y = 40$.

Solution. Since $\gcd(56, 72) = \gcd(16, 56) = \gcd(8, 16) = 8$, this equation simplifies to $7x + 9y = 5$.

Since $\gcd(7, 9) = 1$, we can find $x, y\in\mathbb{Z}$ (for instance using the Euclidean algorithm) such that $7x + 9y = 1$. Indeed, $x = 4$ and $y = -3$ work. Multiplying this with 5, we find that a particular solution to is $7x + 9y = 5$ is provided by $x_0 = 4\cdot 5 = 20$, $y_0 = -3\cdot 5 = -15$.

In conclusion, the general solution is $x = 20 + 9t$, $y = -15 - 7t$, where t is any integer.

Armin Straub
straub@southalabama.edu

Definition 24. Let $a, b \in \mathbb{Z}$ (both not zero). The **least common multiple** $\operatorname{lcm}(a, b)$ of a and b is the smallest positive integer m such that $a|m$ and $b|m$.

Example 25. $\operatorname{lcm}(12, 42) = \operatorname{lcm}(2^2 \cdot 3, 2 \cdot 3 \cdot 7) = 2^2 \cdot 3 \cdot 7 = 84 = \frac{12 \cdot 42}{6}$

Lemma 26. For $a, b \in \mathbb{N}$, $\operatorname{lcm}(a, b) = \frac{ab}{\gcd(a, b)}$.

Proof. Write $d = \gcd(a, b)$ and $m = \frac{ab}{d}$. Note that $a|m$ because $\frac{m}{a} = \frac{b}{d}$ is an integer. Likewise, $b|m$.
Let n be a positive integer such that $a|n$ and $b|n$. (We need to show that $m \leqslant n$. We do that by showing $m|n$.)
Recall that $d = ax + by$ for some integers x, y. Using that, we find that

$$\frac{n}{m} = \frac{nd}{ab} = \frac{n(ax + by)}{ab} = \frac{n}{b}x + \frac{n}{a}y$$

is an integer. That is, $m|n$. □

Example 27. (problem of the "hundred fowls", appears in Chinese textbooks from the 6th century) If a rooster is worth five coins, a hen three coins, and three chicks together one coin, how many roosters, hens, and chicks, totaling 100, can be bought for 100 coins?

Solution. Let x be the number of roosters, y be the number of hens, z be the number of chicks.

$$\begin{aligned} x + y + z &= 100 \\ 5x + 3y + \frac{1}{3}z &= 100 \end{aligned}$$

Eliminating z from the equations by taking $3\mathrm{eq}_2 - \mathrm{eq}_1$, we get $14x + 8y = 200$, or, $7x + 4y = 100$.

- Since 100 is a multiple of $\gcd(7, 4) = 1$, this equation does have integer solutions.
- To find a particular solution, we first spell out Bezout's identity: $7x + 4y = 1$ has $x = -1$, $y = 2$ as a solution. [Make sure that you can find the -1 and 2 using the Euclidean algorithm.]
- Hence, a particular solution to $7x + 4y = 100$ is given by $x = -100$, $y = 200$.
- The homogeneous equation $7x + 4y = 0$ has general solution $x = 4t$, $y = -7t$.
- Hence, the general solution to $7x + 4y = 100$ is $x = -100 + 4t$, $y = 200 - 7t$. These are integers if and only if t is an integer (why?!).
- We can find z using one of the original equations: $z = 100 - x - y = 3t$.
- We are only interested in solutions with $x \geqslant 0$, $y \geqslant 0$, $z \geqslant 0$.
  $x \geqslant 0$ means $t \geqslant 25$. $y \geqslant 0$ means $t \leqslant 28 + \frac{4}{7}$. $z \geqslant 0$ means $t \geqslant 0$.
- Hence, $t \in \{25, 26, 27, 28\}$.
  The four corresponding solutions (x, y, z) are $(0, 25, 75)$, $(4, 18, 78)$, $(8, 11, 81)$, $(12, 4, 84)$.