M 328K: Lecture 3

Katherine Ho

September 3, 2024

1 Problem

If a rooster is worth 5 coins, a hen 3 coins, and 3 chicks together 1 coin, how many roosters, hens, and chicks, totaling 100, can be bought for 100 coins?

$$x = \#roosters$$
$$y = \#hens$$
$$z = \#chicks$$

$$x + y + z = 100$$
$$5x + 3y + \frac{1}{3}z = 100$$

<u>Diophantine Equations</u>

$$x^n + y^n = z^n$$
$$x^2 + y^2 + z^2 + w^2 = n$$

2 Bezout's Theorem

Let $a, b \in \mathbb{Z}$ (not both zero). The gcd of a and b is the smallest positive integer d that can be written as $ax + by = d, x, y \in \mathbb{Z}$.

Proof. Let $S = \{ax + by > 0 | x, y \in \mathbb{Z}\}$. Note that S is nonempty since for $x = a$, $y = b$ we have $ax + by = a^2 + b^2 > 0$. By WOP, S has a smallest element, call it d. WTS:

1. $d|a$, $d|b$
2. if $c|a$, $c|b$, then $c \leq d$

To show $d|a$, apply the division algo to obtain $a = d \cdot q + r, 0 \leq r < d$.
Writing $d = ax_0 + by_0$ for $x_0, y_0 \in \mathbb{Z}$, we have

$$r = a - d \cdot y$$
$$r = a(ax_0 + by_0) \cdot q$$
$$r = a(1 - x_0 q) + b(-y_0 q)$$

Hence, if $r > 0$ then $r \in S$ which is smaller than d, contradicting d being the smallest element. Then, $r = 0$ and $d|a$. (Same argument for $d|b$).
Now suppose that $c \in \mathbb{Z}$ such that $c|a$ and $c|b$. Recall that if x and y are integers, then $c|(cx + by)$. Hence, $c|(ax_0 + by_0) <=> c|d$. Then $c \leq |d| = d$. Therefore, $d = \gcd(a, b)$. $\square$

Corollary 2.1. *Every common divisor of a and b divides* $\gcd(a, b)$.

Corollary 2.2. *The linear Diophantine equation $ax + by = c$ has a solution iff $d|c$.*

Proof. First assume that $ax+by = c$ has a solution: $c = ax_0+by_0$. Since $d|a$, and $d|b$, we have $d|(ax_0+by_0)$.
One the other hand, suppose $d|c$. By definition, $c = d|k$ for some k.
By Bezout's theorem, we can write

$$d = ax + by \text{ for some } x, y \in \mathbb{Z}$$

Then,

$$\begin{aligned} d \cdot k &= a(x \cdot k) + b(y \cdot k) \\ c &= a(x \cdot k) + b(y \cdot k) \end{aligned}$$

So c is an integer linear combo $a < b$ as desired. □

Definition 2.1. *We say that integers a and b (not both zero) are relatively prime or coprime if*

$$\gcd(a, b) = 1$$

Corollary 2.3. *Integers a and b are relatively prime iff there exist $x, y \in \mathbb{Z}$ such that $ax + by = 1$.*

Corollary 2.4. *If a, b are coprime, then $ax + by = c$ has a solution for any $c \in \mathbb{Z}$.*

3 Euclidean Algorithm

1. Start with (a,b) (assume $|a| \geq |b|$)
2. Apply DA: $a = bq + r, 0 \leq r < |b|$
3. If $r = 0$, then $b|a$ and $\gcd(a, b) = |b|$.
4. Otherwise, replace (a, b) with (b, r).
5. Repeat.
6. The final nonzero r is gcd.

Example 3.0.1. $\gcd(12378, 3054)$

$$\begin{aligned} 12378 &= 3054 \cdot 4 + 162 \\ 3054 &= 162 \cdot 18 + 138 \\ 162 &= 138 \cdot 1 + 24 \\ 138 &= 24 \cdot 5 + 18 \\ 24 &= 18 \cdot 1 + 6 \\ 18 &= 6 \cdot 3 + 0 \end{aligned}$$

$$\gcd = 6$$

Note: if you allow for negative remainders, that can be more efficient.

$$\begin{aligned} 3054 &= 162 \cdot 19 - 24 \\ 162 &= (-24)(-7) - 6 \\ -24 &= (-6)(4) + 0 \end{aligned}$$

Example 3.0.2. *Solve $1237x + 3054y = 6$ via "Extended Euclidean Algorithm".*

$$\begin{aligned}
6 &= 24 - 18 \cdot 1 \\
&= 24 - (138 - 24 * 5) \\
&= 24 \cdot 6 - 138 \\
&= (162 - 138) \cdot 6 - 138 \\
&= 162 \cdot 6 - 138 \cdot 7 \\
&= 162 \cdot 6 - (3054 - 162 \cdot 18) \cdot 7 \\
&= (12378 - 3054 \cdot 4) \cdot 6 - (3054 - (12378 - 3054)) \cdot 7
\end{aligned}$$

Example 3.0.3. *Solve*

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

Using $z = 100 - x - y$, we have $7x + 4y = 100$.
Note: $7(-1) + 4(2) = 1$.
So $7(-100) + 4(200) = 100$

$$\begin{aligned}
7 &= 4 \cdot 1 + 3 \\
4 &= 3 \cdot 1 + 1 \\
1 &= 4 - 3 \\
1 &= 4 - (7 - 4) \\
1 &= -7 + 4(2)
\end{aligned}$$

Theorem 3.1. *If $ax + by = c$ has a solution $x_0, y_0 \in \mathbb{Z}$. Then any other solution $x, y \in \mathbb{Z}$ is given by*

$$x = x_0 + \frac{b}{d}k, y = y_0 - \frac{a}{d}k$$

where $k \in \mathbb{Z}$ and $d = \gcd(a, b)$.
If $x, y, z > 0$, then k must satisfy

$$\frac{200}{7} > k > 25$$

So

$$k = 26, 27, 28, \text{ so the only solutions are}$$

$$\begin{aligned}
x &= 4, y = 18, z = 78 \\
x &= 8, y = 11, z = 81 \\
x &= 12, y = -1, z = 89
\end{aligned}$$