Example 44. (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 using the Euclidean algorithm ($\gcd(56, 72) = 8$)
- $56x + 72y = k$ has an integer solution if and only if k is a multiple of $\gcd(56, 72) = 8$

Example 45. (problem of the "hundred fowls", appears in Chinese text books from the 6th century) If a rooster is worth five coins, a hen three coins, and three chickens together one coin, how many roosters, hens, and chickens, 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 chickens.

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

Eliminating z from the equations by taking $3\text{eq}_2 - \text{eq}_1$, 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 $(0, 25, 75)$, $(4, 18, 78)$, $(8, 11, 81)$, $(12, 4, 84)$.

Solving diophantine equations can be incredibly hard!

Example 46. You may have seen Pythagorean triples, which are solutions to the diophantine equation $x^2 + y^2 = z^2$.

A few cases. Some solutions (x, y, z) are $(3, 4, 5)$, $(6, 8, 10)$ (boring! why?!), $(5, 12, 13)$, $(8, 15, 17)$, ...

The general solution. $(m^2 - n^2, 2mn, m^2 + n^2)$ is a Pythagorean triple for any integers m, n.

These solutions plus scaling generate all Pythagorean triples!

For instance, $m = 2, n = 1$ produces $(3, 4, 5)$, while $m = 3, n = 2$ produces $(5, 12, 13)$.

Fermat's last theorem. For, $n > 2$, the diophantine equation $x^n + y^n = z^n$ has no solutions!

Pierre de Fermat (1637) claimed in a margin of Diophantus' book *Arithmetica* that he had a proof ("I have discovered a truly marvellous proof of this, which this margin is too narrow to contain.").

It was finally proved by Andrew Wiles in 1995 (using a connection modular forms and elliptic curves).

This problem is often reported as the one with the largest number of unsuccessful proofs.

Armin Straub
straub@southalabama.edu