**Example 46. (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 $\begin{bmatrix} x \\ y \end{bmatrix} = \begin{bmatrix} 4 \\ -3 \end{bmatrix}$, the general solution is $\begin{bmatrix} x \\ y \end{bmatrix} = \begin{bmatrix} 4 \\ -3 \end{bmatrix} + \begin{bmatrix} 9 \\ -7 \end{bmatrix} t$ where $t \in \mathbb{Z}$.
- $56x+72y=k$ has an integer solution if and only if $k$ is a multiple of $\gcd(56,72)=8$.
- Determine all solutions to the diophantine equation $56x+72y=40$.

  **Solution.** We divide by $\gcd(56,72)=8$ to get $7x+9y=5$.
  As observed above (or by using the Euclidean algorithm), a solution to $7x+9y=1$ is $\begin{bmatrix} x \\ y \end{bmatrix} = \begin{bmatrix} 4 \\ -3 \end{bmatrix}$.
  Hence, the general solution is $\begin{bmatrix} x \\ y \end{bmatrix} = 5\begin{bmatrix} 4 \\ -3 \end{bmatrix} + \begin{bmatrix} 9 \\ -7 \end{bmatrix} t$ where $t \in \mathbb{Z}$.

**Example 47. (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.
- We see (or find using the Euclidean algorithm) that a solution to $7x+4y=1$ is $\begin{bmatrix} x \\ y \end{bmatrix} = \begin{bmatrix} -1 \\ 2 \end{bmatrix}$.
- Hence, $7x+4y=100$ has general solution $\begin{bmatrix} x \\ y \end{bmatrix} = 100\begin{bmatrix} -1 \\ 2 \end{bmatrix} + \begin{bmatrix} 4 \\ -7 \end{bmatrix} t = \begin{bmatrix} -100+4t \\ 200-7t \end{bmatrix}$ where $t \in \mathbb{Z}$.
- 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 $(0,25,75)$, $(4,18,78)$, $(8,11,81)$, $(12,4,84)$.


Armin Straub
straub@southalabama.edu

Solving diophantine equations can be incredibly hard!

**Example 48.** 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 to modular forms and elliptic curves).

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

**Example 49. (HW)** Determine all solutions of $4x + 7y = 67$ with $x$ and $y$ positive integers.

**Solution.** We see that $x = 2$, $y = -1$ is a solution to $4x + 7y = 1$ (you can, of course, use the Euclidean algorithm if you wish).

Hence, a particular solution to $4x + 7y = 67$ is given by $x = 134$, $y = -67$.

The general solution to $4x + 7y = 67$ is thus given by $x = 134 + 7t$, $y = -67 - 4t$, where $t$ can be any integer.

- $x > 0$ if and only if $134 + 7t > 0$ if and only if $t > -\frac{134}{7} \approx -19.14$. That is, $t = -19, -18, \ldots$
- $y > 0$ if and only if $-67 - 4t > 0$ if and only if $t < -\frac{67}{4} = -16.75$. That is, $t = -17, -18, \ldots$

Hence, we get a solution $(x, y)$ with positive integers $x$, $y$ for $t = -19, -18, -17$. The three corresponding solutions are: $(1, 9)$, $(8, 5)$, $(15, 1)$.

## 5 Congruences

$$a \equiv b \pmod{n} \qquad \text{means} \qquad a = b + mn \quad (\text{for some } m \in \mathbb{Z})$$

In that case, we say that "$a$ is congruent to $b$ modulo $n$".

- In other words: $a \equiv b \pmod{n}$ if and only if $a - b$ is divisible by $n$.
- In yet other words: $a \equiv b \pmod{n}$ if and only if $a$ and $b$ leave the same remainder when dividing by $n$.

**Example 50.** $17 \equiv 5 \pmod{12}$ as well as $17 \equiv 29 \equiv -7 \pmod{12}$

**Example 51.** We will discuss in more detail that, and how, we can calculate with congruences.

Here is an appetizer: What is $2^{100}$ modulo $3$? That is, what's the remainder upon division by $3$?

**Solution.** $2 \equiv -1 \pmod{3}$. Hence, $2^{100} \equiv (-1)^{100} = 1 \pmod{3}$.

**Theorem 52.** We can calculate with congruences.

- First of all, if $a \equiv b \pmod{n}$ and $b \equiv c \pmod{n}$, then $a \equiv c \pmod{n}$.

  In other words, being congruent is a **transitive property**.

  **Why?** $n|(b-a)$ and $n|(c-b)$, then $n|\underbrace{((b-a)+(c-b))}_{=c-a}$.

  Alternatively, we can note that each of $a, b, c$ leaves the same remainder when dividing by $n$.

- If $a \equiv b \pmod{n}$ and $c \equiv d \pmod{n}$, then

  (a) $a + c \equiv b + d \pmod{n}$

  **Why?** $(b+d) - (a+c) = (b-a) + (d-c)$ is indeed divisible by $n$ (because $n|(b-a)$ and $n|(d-c)$).

  (b) $ac \equiv bd \pmod{n}$

  **Why?** $bd - ac = (bd - bc) + (bc - ac) = b(d-c) + c(b-a)$ is indeed divisible by $n$ (because $n|(b-a)$ and $n|(d-c)$).

- In particular, if $a \equiv b \pmod{n}$, then $a^k \equiv b^k \pmod{n}$ for any positive integer $k$.

**Example 53.** Compute $36 \cdot 75 \pmod{11}$.

**Solution.** Since $36 \equiv 3 \pmod{11}$ and $75 \equiv -2 \pmod{11}$, we have $36 \cdot 75 \equiv 3 \cdot (-2) = -6 \equiv 5 \pmod{11}$.

**Important comment.** We do not need to compute that $36 \cdot 75 = 2700$ (and then reduce modulo $11$)! Our ability to avoid computing large intermediate quantities is crucial for applications like cryptography.