1. LDEs
2. Congruences

$ax+by=c$

(x_0, y_0) is one soln.

$\{(x_0+\frac{b}{d}n, y_0-\frac{a}{d}n) \mid n\in\mathbb{Z}\}$

Example: $119x+84y=777$ $\quad \gcd(119,84)=7$

$119\cdot555+84\cdot(-777)=777$

Complete sol^n: $\{(555+12n, -777-17n) \mid n\in\mathbb{Z}\}$

$n=1: (567, -794)$

$n=-1: (543, -760)$

$n=10000: (120555, -170777)$

Are there positive integer solutions?

Solve $555+12n>0$, $-777-17n>0$

$n>-\frac{555}{12}=-46.25 \qquad n<-\frac{777}{14}\approx 45.7$

So $n=-46$ is the only possibility.

$(555+12(-46), -777-17(-46))=(3,5)$

Congruences

Definition: Let $m \in \mathbb{N}$ be fixed, $a, b \in \mathbb{Z}$. Then <u>a is congruent to b module m</u> if $m \mid (a-b)$.

Notation: $a \equiv b \pmod{m}$. Otherwise $a \equiv b \pmod{m}$.

Alternatively: $a - b = km$ for some $k \in \mathbb{Z}$

$$a = b + km$$

Example: $m=7$. $2 \equiv 9 \pmod{7}$ $\quad 7 \mid (2-9)$

$1 \equiv 9 \pmod{7}$ $\quad 7 \nmid (1-9)$

$59 \equiv 31 \pmod{7}$ $\quad 7 \mid (59-31)$

For which m is $59 \equiv 31 \pmod{m}$? $\quad m \mid 28$

$m = 1, 2, 4, 7, 14, 28.$

Definition: A relation $\sim$ is an equivalence relation if it is reflexive, symmetric, and transitive.

Proposition: $\equiv$ is an equivalence relation.

Let $m \in \mathbb{N}$, $a, b, c \in \mathbb{Z}$, then

① (reflexive) $a \equiv a \pmod{m}$

② (symmetric) if $a \equiv b \pmod{m}$, then $b \equiv a \pmod{m}$

③ (transitive) if $a \equiv b \pmod{m}$ and $b \equiv c \pmod{m}$, then $a \equiv c \pmod{m}$

Proof: ① $a-a=0$ and $m|0$. So $a \equiv a \pmod m$

② Since $m|(a-b)$, $m|-(a-b)$, so $m|(b-a)$

So $b \equiv a \pmod m$

③ Since $a \equiv b \pmod m$, $m|(a-b)$

Since $b \equiv c \pmod m$, $m|b-c)$

By DIC, $m|[(a-b)+(b-c)]$,

so $m|(a-c)$.

So $a \equiv c \pmod m$.

If $\sim$ is an eq. rel, the universe can be partitioned into "equivalence classes" where within a class, every pair of elements is related, and elements in different classes are not related.

For $\equiv \pmod 5$, the integers congruent to 0 are

$\ldots -10, -5, 0, 5, 10, 15, 20, \ldots$ Any 2 are cong

$$\left.\begin{array}{l} -5 \equiv 0 \pmod 5 \\ 0 \equiv 20 \pmod 5 \end{array}\right] \to -5 \equiv 20 \pmod 5$$

Define $[0] = \{5n \mid n \in \mathbb{Z}\}$

$[1] = \{5n+1 \mid n \in \mathbb{Z}\} = \{\ldots, -9, -4, 1, 6, 11, 16, \ldots\}$

$[2] = \{5n+2 \mid n \in \mathbb{Z}\}$

$[3] = \{5n+3 \mid n \in \mathbb{Z}\}$ These are the

$[4] = \{5n+4 \mid n \in \mathbb{Z}\}$ equivalence classes for $\equiv \pmod 5$

Example: define $A \heartsuit B$ if A, B are in the same eng. class.

This is an eq. rel. Ted $\heartsuit$ Ted

Equivalence classes: eng depts.