Lesson 22

Linear congruences: more examples

Recall:

Given the diophantine equation

$$(*) \quad ax + by = c$$

Let $d = (a, b)$

① $(*)$ has solutions $\iff$ d div c

② If $(*)$ has solutions, it has infinitely many. The solutions are:

$$x = x_1 + \frac{b}{d}n \qquad y = y_1 - \frac{a}{d}n \qquad n \in \mathbb{Z}$$

where $x = x_1$ $y = y_1$ is one solution

③ To find x_1 and y_1 We use the Euclideen algorithm (backwards) to write d as $ax_0 + by_0 = d$

if $c = dk$ we multiply by k.

$$\underbrace{a(x_0 k)}_{x_1} + b\underbrace{(y_0 k)}_{y_1} = \underbrace{dk}_{c}$$

$(**)$ $\quad ax \equiv_m b$

The solutions to $(**)$ are the "x part" of the solutions to the associated linear diophantine equation

$$ax + my = b$$

$$x = x_1 + \frac{m}{d} n \qquad n \in \mathbb{Z}$$

$$d = (a, m)$$

$(**)$ has solutions $\Leftrightarrow$ d div b

if it has solutions it has

a) infinitely many integer solutions

b) d solutions in $\mathbb{Z}_m$

Solve $290x \equiv_{357} 5$

1) Cancel 5 $\quad 58x \equiv_{357} 1$

2) Associated linear diophantine equation:

$58x + 357y = 1$

3) Compute $(58 \quad 357)$

using Euclidean algorithm

$357 = 58 \times 6 + 9$

$58 = 9 \times 6 + 4$

$9 = 4 \times 2 + 1$

$4 = 1 \times 4 + 0$

4) $(58, 357) = 1 \qquad 1 \text{ div } 1$

So infinitely many solutions in $\mathbb{Z}$

$d=1$ solution in $\mathbb{Z}_{357}$

5) Write 1 as a linear combination of 58 and 357:

$1 = 9 - 4 \times 2$

$1 = 9 - (58 - 9 \times 6) \times 2 = 9 \times (13) + 58(-2)$

$1 = (357 - 58 \times 6) \times 13 + 58(-2) = 357 \times 13 + 58(-80)$

$y_1 \qquad x_1$

5) Keep x part : $x_1 = -80$

6) Integer solutions to $58x \equiv_{357} 1$ are $-80 + 357n \quad n \in \mathbb{Z}$

Solution in $\mathbb{Z}_{357}$ $-80 + 357 = 277$

Example

Solve $102x \equiv 10 \mod 1001$

1) $(102, 1001)$ divides 10 ?

Note: I could have cancelled 2

Compute $(102, 1001)$ using Euclidean algorithm:

Calculate $d = (102, 1001)$.

$$\begin{aligned} 1001 &= 9 \times 102 + 83 \\ 102 &= 1 \times 83 + 19 \\ 83 &= 4 \times 19 + 7 \\ 19 &= 2 \times 7 + 5 \\ 7 &= 1 \times 5 + 2 \\ 5 &= 2 \times 2 + 1 \\ 2 &= 2 \times 1 + 0 \end{aligned}$$

$$d = 1$$

1 div 10 so infinitely many solutions in $\mathbb{Z}$. 1 solution in $\mathbb{Z}_{1001}$

How do I find solutions?

$$102\,x_1 \equiv 10 \mod 1001$$

$$\Leftrightarrow$$

$$1001 \text{ div } 102\,x_1 - 10$$

$$\Leftrightarrow$$

$$102\,x_1 - 10 = 1001\,k$$

$$\Leftrightarrow$$

$$102\,x_1 - 1001\,k = 10$$

$$\Leftrightarrow$$

$$102\,x_1 + 1001\,y_1 = 10 \qquad y_1 = -k$$

$$\Leftrightarrow$$

x_1 y_1 is a solution of

$$102\,x + 1001\,y = 10$$

Associated linear diophantine equation

$= (102, 1001)$

2) Write 1 as a linear combination of 102 and 1001

From Euclidean algorithm, bottom to top

$$1 = 5 - 2 \times 2$$

$$1 = 5 - 2 \times (7 - 5) = -2 \times 7 + 3 \times 5$$

$$1 = -2 \times 7 + 3 \times (19 - 2 \times 7) = 3 \times 19 - 8 \times 7$$

$$1 = 3 \times 19 - 8 \times (83 - 4 \times 19) = 35 \times 19 - 8 \times 83$$

$$1 = -8 \times 83 + 35 \times (102 - 83) = 33 \times 102 - 43 \times 83$$

$$1 = 35 \times 102 - 43 \times (1001 - 9 \times 102) =$$

$$= -43 \times 1001 + 422 \times 102$$

Therefore: $102 \times 422 + 1001(-43) = 1$

Multiply both sides by 10

$$102 \times \underbrace{422 \cdot 10}_{x_1} + 1001 \cdot \underbrace{(-43 \cdot 10)}_{y_1} = 10$$

Therefore one particular solution of $102x + 1001y = 10$ is

$x_1 = 4220$, $y_1 = -430$

All solutions are given by

$x = 4220 + \frac{1001}{1}k$, $y = -430 - \frac{102}{1}k$

$k \in \mathbb{Z}$

Back to $102 \equiv 10 \mod 1001$ sol in $\mathbb{Z}$ are $4220 + 1001k$ $k \in \mathbb{Z}$

in $\mathbb{Z}_{1001}$ only one solution

$4220 - 4004 = 216$

Find all integers x s.t.

$$6^{411} \cdot x + 8^{911} + 2 = 2^{36} \mod 7$$

1) Put in standard form $ax \equiv b \mod 7$

$6 \equiv -1 \mod 7$

$8 \equiv 1 \mod 7$

$2^{36} = (2^3)^{12} \equiv 1^{12} \mod 7$

$-x + 1 + 2 \equiv 1 \mod 7$

$-x + 3 \equiv 1 \mod 7$

2) Can I subtract 3 from both sides?
Can I multiply both sides by -1?

$-x \equiv -2 \mod 7$

$x \equiv 2 \mod 7$

3) $x = 2 + 7k \quad k \in \mathbb{Z}$

Th (1) $ax \equiv_m b$ and

(2) $ax + c \equiv_m b + c$

have the same solutions

Proof: Suppose $x = x_1$ is

a solution to (1), then

$ax_1 \equiv_m b$; certainly $c \equiv_m c$ so

$ax_1 + c \equiv b + c$ so x_1 is a

solution to $ax + c \equiv_m b + c$

Vice versa suppose x_2 is a

solution to (2) then

$ax_2 + c \equiv_m b + c$; certainly $-c \equiv_m -c$

so $ax_2 + c - c \equiv b + c - c$ so

x_2 is a solution to $ax \equiv_m b$

Do $ax \equiv_m b$ and

$cx \equiv_m b$ have

The same solutions ?

No $2x \equiv_4 2$ has

solutions $x = 1, 3$ in $\mathbb{Z}_4$

or

$x = 1 + 4n \quad n \in \mathbb{Z}$

$x = 3 + 4n \quad n \in \mathbb{Z}$

in $\mathbb{Z}$

but $2 \cdot 2x \equiv_4 2 \cdot 2$

has solutions $x = 0, 1, 2, 3$

in $\mathbb{Z}_4$ or

all $n \in \mathbb{Z}$ in $\mathbb{Z}$

Consider (1) $ax \equiv_m b$ and

(2) $cax \equiv_{cm} cb$

Suppose x_1 is a solution to (1) then $ax_1 \equiv_m b$; certainly $c \equiv_m c$ so $cax_1 \equiv_{cm} cb$ so

x_1 is a solution to (1)

Suppose x_2 is a solution to (2) then $cax_2 \equiv_{cm} cb$ can I cancel c? If I do I have to change module to $\frac{m}{(m,c)}$

Th: When $(c, m) = 1$

(1) $ax \equiv_m b$ and

(2) $cax \equiv_{cm} cb$

have the same solutions