Linear congruences and the Chinese remainder theorem

LET $a, b \in \mathbb{Z}$, $m \in \mathbb{N}$. AN EQUATION OF THE FORM $ax \equiv_m b$ IS CALLED A LINEAR CONGRUENCE, AND BY A SOLUTION OF SUCH AN EQUATION WE MEAN AN INTEGER x_0 FOR WHICH $a x_0 \equiv_m b$.

BY DEFINITION, $a x_0 \equiv_m b$ IFF $m \mid a x_0 - b$ IFF $a x_0 - b = m y_0$ FOR SOME $y_0 \in \mathbb{Z}$. THUS, THE PROBLEM OF FINDING ALL INTEGERS THAT WILL SATISFY THE LINEAR CONGRUENCE $ax \equiv_m b$ IS IDENTICAL WITH THAT OF OBTAINING ALL SOLUTIONS OF THE LINEAR DIOPHANTINE EQUATION $ax - my = b$.

IT IS CONVENIENT TO TREAT TWO SOLUTIONS OF $ax \equiv_m b$ THAT ARE CONGRUENT MODULO m AS BEING 'EQUAL' EVEN THOUGH THEY ARE NOT EQUAL IN THE USUAL SENSE. SO, WHEN WE REFER TO THE NUMBER OF SOLUTIONS OF $ax \equiv_m b$, WE MEAN THE NUMBER OF INCONGRUENT INTEGERS SATISFYING THIS CONGRUENCE.

THEOREM: THE LINEAR CONGRUENCE $ax \equiv_m b$ HAS A SOLUTION IF AND ONLY IF $d \mid b$, WHERE $d = \gcd(a, m)$. IF $d \mid b$ THEN IT HAS d MUTUALLY INCONGRUENT SOLUTIONS MODULO m.

GIVEN $a, b \in \mathbb{Z}$, $m \in \mathbb{N}$, WE WANT TO FIND ALL $x \in \mathbb{Z}$ SUCH THAT $ax \equiv_m b$. NOTE THERE EXISTS $x \in \mathbb{Z}$ SUCH THAT $ax \equiv_m b$ IFF $m \mid ax - b$ IFF THERE EXIST $x, y \in \mathbb{Z}$ SUCH THAT $ax - b = ym$ IFF THERE EXIST $x, y \in \mathbb{Z}$ SUCH THAT $ax + (-m)y = b$ IFF THE EQUATION $ax + (-m)y = b$ HAS A SOLUTION IFF $\gcd(a, -m) = \gcd(a, m)$ DIVIDES b. FOR EXAMPLE, THE EQUATION $14x \equiv_{21} 5$ HAS NO SOLUTIONS SINCE $\gcd(14, 21) = 7$ AND $7 \nmid 5$.

LET $d = \gcd(a, m)$. SUPPOSE THAT $d \mid b$. WE WANT TO SOLVE $ax \equiv_m b$. TO DO THIS WE COULD FIND ALL $x, y \in \mathbb{Z}$ SUCH THAT $ax + (-m) \cdot y = b$. THEN, ALL $x \in \mathbb{Z}$ WE FIND ARE ALL THE SOLUTIONS OF $ax \equiv_m b$.

EXERCISE 1: SOLVE $36x \equiv_{102} 8$ AND $34x \equiv_{98} 60$ IF POSSIBLE.

SOLUTION: WE FIRST OBSERVE, $\gcd(36, 102) = \gcd(102, 36) = \gcd(36, 30) = \gcd(30, 6) = 6$. THEN, SINCE $6 \nmid 8$ THE EQUATION $36x \equiv_{102} 8$ HAS NO SOLUTION. ON THE OTHER HAND, NOTE $\gcd(34, 98) = \gcd(2 \cdot 17, 2 \cdot 49) = 2 \cdot \gcd(17, 49) = 2$. AS $2 \mid 60$, THE EQUATION $34x \equiv_{98} 60$ HAS INTEGERS SOLUTIONS. NOTE

$$34x \equiv_{98} 60 \iff 2 \cdot 17x \equiv_{98} 2 \cdot 30 \iff 17x \equiv_{\frac{98}{2}} 30 \iff 17x \equiv_{49} 30.$$

$$\iff 49 \mid 17x - 30 \iff 17x + (-49)y = 30 \text{ HAS INTEGER SOLUTIONS.}$$

NOW, WE SOLVE THIS DIOPHANTINE EQUATION. WE OBSERVE

$$49 = 17 \cdot 2 + 15, \quad 17 = 15 \cdot 1 + 2, \quad 15 = 7 \cdot 2 + 1. \text{ THIS SHOWS}$$

$$1 = 15 - 7 \cdot 2 = 15 - 7 \cdot (17 - 15) = 8 \cdot 15 - 7 \cdot 17 = 8(49 - 17 \cdot 2) - 7 \cdot 17$$
$$= 8 \cdot 49 - 17 \cdot 16 - 7 \cdot 17 = 8 \cdot 49 - 23 \cdot 17 = 17 \cdot (-23) + (-49) \cdot (-8).$$

THEN, $17 \cdot (-23) \cdot 30 + (-49) \cdot (-8) \cdot 30 = 30$ SHOWS $(x, y) = (-690, 11760)$ IS A SOLUTION. THEN, ANY OTHER SOLUTION HAS THE FORM $x = -690 + 49t$ FOR SOME CHOICE OF $t \in \mathbb{Z}$. THEN, THE INTEGERS $x = -690 + 49t$ FOR $t = 0, 1$ ARE INCONGRUENT MODULO 98 (BUT ALL OF THEM ARE CONGRUENT MODULO 49). THEN THE INCONGRUENT SOLUTIONS ARE $x \equiv_{98} -690$ AND $x \equiv_{98} -641$. EQUIVALENTLY, $x \equiv_{98} 94$ AND $x \equiv_{98} 45$. $\blacksquare$

WE NEXT SEE ANOTHER WAY TO SOLVE LINEAR CONGRUENCES.

SINCE $d \mid a$, $d \mid b$, $d \mid m$ THEN $\frac{a}{d}, \frac{b}{d}, \frac{m}{d}$ ARE ALL INTEGERS. THEN,

$$aX \equiv_m b \iff d.\frac{a}{d}X \equiv_{d.\frac{m}{d}} d.\frac{b}{d} \iff \frac{a}{d}X \equiv_{\frac{m}{d}} \frac{b}{d}.$$

SINCE $\gcd\left(\frac{a}{d}, \frac{m}{d}\right) = 1$ THEN THERE EXIST $s, t \in \mathbb{Z}$ SUCH THAT

$1 = k.\frac{a}{d} + s.\frac{m}{d}$. THIS SHOWS THAT $1 \equiv_{\frac{m}{d}} k.\frac{a}{d}$. MOREOVER,

$$\frac{a}{d}X \equiv_{\frac{m}{d}} \frac{b}{d} \iff \frac{a}{d}kX \equiv_{\frac{m}{d}} \frac{b}{d}k \iff 1.X \equiv_{\frac{m}{d}} \frac{b}{d}k \iff X \equiv_{\frac{m}{d}} \frac{b}{d}k,$$

AS THE INTEGERS k AND $\frac{m}{d}$ ARE COPRIMES.

WE THUS HAVE $X \equiv_{\frac{m}{d}} X_0$ WHERE X_0 IS THE REMAINDER OF $\frac{b}{d}k$ IN THE DIVISION BY $\frac{m}{d}$. FURTHERMORE, ALL THE SOLUTIONS ARE $X = X_0 + t.\frac{m}{d}$ WHERE $t \in \mathbb{Z}$ AND $0 \leq t \leq d-1$.

EXERCISE 2: FIND ALL $x \in \mathbb{Z}$ SUCH THAT $39X \equiv_{45} 24$.

SOLUTION: WE FIRST OBSERVE $\gcd(39, 45) = 3$ AND $3 | 24$. SO, THE GIVEN EQUATION HAS SOLUTIONS. NOTE ALSO THAT $39X \equiv_{45} 24 \iff 13X \equiv_{15} 8$. NOTE THAT $\gcd(13, 15) = 1$. MOREOVER, IT IS EASY TO SEE $1 = 7.13 + (-6).15$ WHICH IMPLIES $7.13 \equiv_{15} 1$. THEN, SINCE 7 AND 15 ARE COPRIME,

$$13X \equiv_{15} 8 \iff 7.13X \equiv_{15} 7.8 \iff X \equiv_{15} 56 \iff X \equiv_{15} 11.$$

THEN, THE SOLUTIONS ARE $X = 11 + 15t$ FOR SOME $t \in \mathbb{Z}$. NOTE THE INTEGERS $X = 11 + 15t$ WITH $t \in \{0, 1, 2\}$ ARE INCONGRUENT MODULO 45. SO, THE SOLUTIONS ARE $X \equiv_{45} 11$, $X \equiv_{45} 26$ AND $X \equiv_{45} 41$.

EXERCISE 3: FIND ALL $a \in \mathbb{Z}$ SUCH THAT $\gcd(7a+2, 5a+3) \neq 1$.

SOLUTION: LET $d = \gcd(7a+2, 5a+3)$. THEN, $d | 7a+2$ AND $d | 5a+3$. NOTE THAT

$$\begin{cases} d | (7a+2).5 \\ d | (5a+3).7 \end{cases} \Rightarrow \begin{cases} d | 35a+10 \\ d | 35a+21 \end{cases} \Rightarrow d | (35a+21) - (35a+10) \Rightarrow d | 11.$$

THEN, EITHER $d=1$ OR $d=11$. OBSERVE $d=11$ IFF $11 \mid 7a+2$, $11 \mid 5a+3$. WE FIRST FIND $a \in \mathbb{Z}$ SUCH THAT $11 \mid 7a+2$. OBSERVE

$$11 \mid 7a+2 \iff 7a+2 \equiv_{11} 0 \iff 7a \equiv_{11} -2 .$$

AS 7 AND 11 ARE COPRIME, THIS LINEAR CONGRUENCE HAS SOLUTIONS. NOTE THAT $1 = 7.(-3) + 11.2$. THEN $7.(-3) \equiv_{11} 1$. SO,

$$7a \equiv_{11} -2 \iff (-3).7a \equiv_{11} (-3)(-2) \iff a \equiv_{11} 6 \quad \text{AS} \quad \gcd(-3,11)=1.$$

SIMILARLY, WE OBSERVE $11 \mid 5a+3 \iff 5a+3 \equiv_{11} 0 \iff 5a \equiv_{11} -3$. NOTE $1 = 5.(-2) + 11.1$ AND $5.(-2) \equiv_{11} 1$. THEN, AS $\gcd(-2,11)=1$,

$$5a \equiv_{11} -3 \iff 5.(-2)a \equiv_{11} (-3)(-2) \iff a \equiv_{11} 6.$$

THEREFORE, ALL $a \in \mathbb{Z}$ SUCH THAT $\gcd(7a+2, 5a+3) \neq 1$ ARE ALL OF THE FORM $a = 6 + 11q$, $q \in \mathbb{Z}$.

EXERCISE 4: LET $a,b,c \in \mathbb{Z}$, $m \in \mathbb{N}$ SUCH THAT $\gcd(c,m)=1$. PROVE THAT $ac \equiv_m bc$ IFF $a \equiv_m b$.

SOLUTION: SUPPOSE FIRST THAT $ac \equiv_m bc$. THEN, $m \mid ac-bc$ WHICH MEANS THAT $m \mid c(a-b)$. SINCE m AND c ARE COPRIME, IT FOLLOWS $m \mid a-b$ AND SO, $a \equiv_m b$. SUPPOSE NEXT THAT $a \equiv_m b$. THEN $m \mid a-b$ AND SO, $m \mid c(a-b) = c.a - cb$. THIS SHOWS THAT $ac \equiv_m cb$. OBSERVE THIS PROPERTY WAS USED IN THE PREVIOUS EXERCISES!

EXERCISE 5: FIND THE SOLUTION OF THE LINEAR CONGRUENCE SYSTEM

$$\begin{cases} 2x \equiv_{35} -7 \\ 5x \equiv_{26} -1 \end{cases}$$

SOLUTION: SUPPOSE WE WANT TO FIND ALL INTEGERS $x \in \mathbb{Z}$ SUCH THAT

$2X \equiv_{35} -7$ AND $5X \equiv_{26} -1$. SINCE $\gcd(2,35) = \gcd(5,26) = 1$,

$$2X \equiv_{35} -7 \iff 2X \equiv_{35} 28 \iff X \equiv_{35} 14.$$

$$5X \equiv_{26} -1 \iff 5X \equiv_{26} 25 \iff X \equiv_{26} 5.$$

THEN, IT IS EQUIVALENT TO FIND ALL $x \in \mathbb{Z}$ SUCH THAT $X \equiv_{35} 14$ AND $X \equiv_{26} 5$.
OBSERVE, $x \in \mathbb{Z}$ IS A SOLUTION OF THE SYSTEM IFF $X = 35k + 14$ AND $35k + 14 \equiv_{26} 5$ IFF $X = 35k + 14$ AND $35k \equiv_{26} -9$. SINCE $\gcd(35, 26) = 1$ AND $1 \mid 9$ WE NOTE THERE EXISTS $k \in \mathbb{Z}$ SUCH THAT $35k \equiv_{26} -9$. THEN, $35k \equiv_{26} -9 \iff 9k \equiv_{26} -9 \iff k \equiv_{26} -1$ SINCE $\gcd(9, 26) = 1$. THEN, $35k \equiv_{26} -9 \iff k = 26q - 1$, $q \in \mathbb{Z}$. THUS, X IS A SOLUTION IFF $X = 35k + 14$ AND $k = 26q - 1$ FOR SOME $q \in \mathbb{Z}$ IFF $X = 35(26q - 1) + 14$ IFF $X = 35.26.q - 21$, $q \in \mathbb{Z}$. NOTE THAT THERE IS SOLUTION SINCE $\gcd(35, 26) = 1$.

SUPPOSE NOW WE WANT TO SOLVE THE SYSTEM $\begin{cases} 7X \equiv_{30} 1 \\ 5X \equiv_{31} 84 \end{cases}$. IT IS EASY TO SEE THE ABOVE SYSTEM IS EQUIVALENT TO $\begin{cases} X \equiv_{30} 13 \\ X \equiv_{23} 84 \end{cases}$. THEREFORE, $x \in \mathbb{Z}$ IS A SOLUTION IFF $X = 30k + 13$ AND $30k + 13 \equiv_{84} 23$ IFF $X = 30k + 13$ AND $30k \equiv_{84} 10$.
WE NOW OBSERVE $\gcd(30, 84) = 6$ AND $6 \nmid 10$. THEN, THERE IS NO SOLUTION.
NOTE HERE $\gcd(30, 84) \neq 1$ AND THERE IS NO SOLUTION.

WE NOW CONSIDER THE SYSTEM $\begin{cases} 3X \equiv_{14} 13 \\ 7X \equiv_{20} -13 \end{cases}$. IT IS EASY TO SEE THAT THIS SYSTEM IS EQUIVALENT TO THE SYSTEM $\begin{cases} X \equiv_{14} 9 \\ X \equiv_{20} 1 \end{cases}$. WE THUS HAVE $x \in \mathbb{Z}$ IS A SOLUTION IFF $X = 14k + 9$ AND $14k + 9 \equiv_{20} 1$ IFF $X = 14k + 9$ AND $14k \equiv_{20} -8$. WE OBSERVE $\gcd(14, 20) \mid -8$ AND SO THERE EXISTS SUCH $k \in \mathbb{Z}$. IT TURNS OUT THAT ALL THE SOLUTIONS ARE $X = 10.14q - 19$.
NOTE HERE $\gcd(14, 20) \neq 1$ AND THERE ARE SOLUTIONS.

IN GENERAL, A LINEAR CONGRUENCE SYSTEM IS ALWAYS EQUIVALENT TO A SYSTEM

OF THE FORM $\begin{cases} x \equiv_{m_1} a_1 \\ x \equiv_{m_2} a_2 \end{cases}$. MOREOVER, IF $\gcd(m_1, m_2) = 1$ THEN THE SYSTEM HAS SOLUTION. IF $\gcd(m_1, m_2) \neq 1$ THEN BOTH CASES ARE POSSIBLE : TO HAVE A SOLUTION OR NOT.

THEOREM: (CHINESE REMAINDER THEOREM) LET $m_1, m_2, \ldots, m_r$ BE POSITIVE INTEGERS SUCH THAT $\gcd(m_i, m_j) = 1$ FOR $i \neq j$. THEN THE SYSTEM OF LINEAR CONGRUENCES

$$x \equiv_{m_1} a_1$$
$$x \equiv_{m_2} a_2$$
$$\vdots$$
$$x \equiv_{m_r} a_r$$

HAS A SIMULTANEOUS SOLUTION, WHICH IS UNIQUE MODULO THE INTEGER $M = m_1 m_2 \ldots m_r$. MOREOVER, FOR EACH $1 \leq k \leq r$, LET $N_k = \frac{M}{m_k}$ AND SO $\gcd(N_k, m_k) = 1$. THEN, THE EQUATION $N_k x \equiv_{m_k} 1$ HAS A UNIQUE SOLUTION x_k AND THE NUMBER $\bar{x} = a_1 N_1 x_1 + a_2 N_2 x_2 + \ldots + a_r N_r x_r$ IS A SIMULTANEOUS SOLUTION OF THE GIVEN SYSTEM.

EXERCISE 6: FIND THE SOLUTION OF THE SYSTEM

$$x \equiv_4 1, \quad x \equiv_7 2 \quad \text{AND} \quad x \equiv_{15} 4.$$

SOLUTION: NOTE THAT $\gcd(4, 7, 15) = 1$. SO, THE GIVEN SYSTEM HAS A SOLUTION MODULO $M = 4.7.15 = 420$. LET $m_1 = 4$, $m_2 = 7$, $m_3 = 15$. THEN $N_1 = 7.15 = 105$, $N_2 = 4.15 = 60$, $N_3 = 4.7 = 28$ AND $a_1 = 1$, $a_2 = 2$, $a_3 = 4$.
WE NOW SOLVE $N_1 x \equiv_{m_1} 1$, $N_2 x \equiv_{m_2} 1$ AND $N_3 x \equiv_{m_3} 1$. THEN,

$$N_1 x \equiv_{m_1} 1 \iff 105 x \equiv_4 1 \iff x \equiv_4 1$$

$N_2 x \equiv_{m_2} 1 \iff 60x \equiv_7 1 \iff 4x \equiv_7 1 \iff 8x \equiv_7 2 \iff x \equiv_7 2.$

$N_3 x \equiv_{m_3} 1 \iff 28x \equiv_{15} 1 \iff -2x \equiv_{15} 1 \iff 16x \equiv_{15} -8 \iff x \equiv_{15} 7.$

THEN, WE CAN TAKE $x_1 = 1$, $x_2 = 2$, $x_3 = 7$. SO, WE GET

$\bar{x} = a_1 N_1 x_1 + a_2 N_2 x_2 + a_3 N_3 x_3 = 1.105.1 + 2.60.2 + 4.28.7 = 1129.$

WE THUS HAVE $x = 1129 \equiv_{420} 289$. THEN, ALL SOLUTIONS ARE

$x = 420q + 289, \quad q \in \mathbb{Z}.$