Section 5 — Linear Congruences

Want to solve $ax \equiv b \pmod{m}$.

Q: How many solutions do you expect?

...and what do we mean by "solution"?

Ex Find all solutions to $3x \equiv 6 \pmod{10}$.

Thm 4 – Sect. 4 : $\boxed{(3,10)=1}$ so we can cancel.

$3x \equiv 6 \pmod{10} \iff x \equiv 2 \pmod{10}$

Answer 1 : $\boxed{x \equiv 2 \pmod{10}}$ 1 solution

Answer 2 : $x = 2, 12, 22, \ldots \quad -8, -18, \ldots$

so, $\boxed{x = 2 + 10t \text{ for } t \in \mathbb{Z}.}$ ∞-many sol.

Convention: when we talk about solutions to a congruence (e.g. $ax \equiv b \pmod{m}$) we will only consider least residues mod m.

Ex Find all solutions.

(a) $3x \equiv 6 \pmod{7}$ cancel — 3 is cancellable modulo 7

(b) $3x \equiv 1 \pmod{7}$ $3x \equiv 8 \equiv 15$ ... now cancel

(c) $3x \equiv 1 \pmod{6}$

(d) $3x \equiv 3 \pmod{6}$

$\}$ table. (3 is not cancellable modulo 6)

Lemma x_0 is a solution to $ax \equiv b \pmod{m}$ iff for some $y_0 \in \mathbb{Z}$, x_0, y_0 is a solution to $ax + my = b$.

pf

$$ax_0 \equiv b \pmod{m} \iff m \mid (ax_0 - b)$$
$$\iff ax_0 - b = km \quad \text{for some } k \in \mathbb{Z}$$
$$\iff ax_0 + m(-k) = b \qquad {}^{\shortparallel}\ y_0$$
$$\iff x_0, -k \text{ is a solution to } ax + my = b$$

$\square$

Find all (least residue) solutions to $ax \equiv b \pmod{m}$	$\longleftrightarrow$	Find all x-values of the solutions to $ax + my = b$ with $0 \le x < m$.

Theorem 1 Consider $ax \equiv b \pmod{m}$. Let $d = (a, m)$.

① If $d \nmid b$, then there are no solutions.

② If $d \mid b$, then there are exactly d solutions.
counting only least residues.

pf idea

solutions to $ax \equiv b \pmod{m}$ $\longleftrightarrow$ x-values of solutions to $ax + my = b$, $0 \le x < m$

① If $d \nmid b$, there are no solutions by Lemma 2 – Sect. 3.

Optional

② Assume $d \mid b$. Note that $d \mid a$, $d \mid m$, $d \mid b$ so $ax + my = b$ is not reduced.

optional

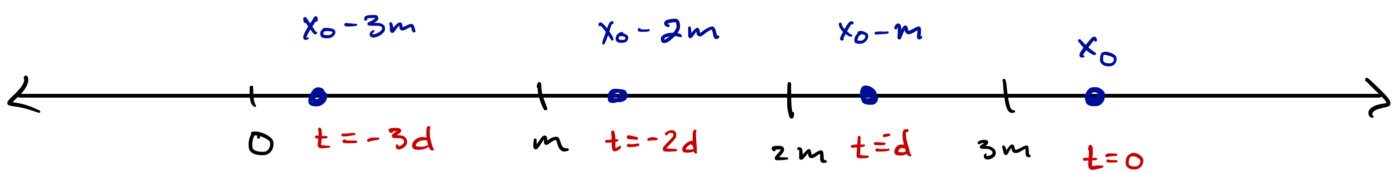
However,

$$\frac{a}{d}x + \frac{m}{d}y = \frac{b}{d}$$

is reduced. Let x_0, y_0 be one sol. Then all solutions are given by

$$x = x_0 + \frac{m}{d}t \qquad t \in \mathbb{Z}.$$
$$y = y_0 - \frac{a}{d}t$$

we want solutions with $0 \le x < m$.



Thus for some value of t, there is a solution with $0 \le x < m$. Let x_1, y_1 be a solution with x_1 positive and as small as possible. Rewrite the solutions to $\frac{a}{d}x + \frac{m}{d}y = \frac{b}{d}$ as

$$x = x_1 + \frac{m}{d}s \qquad s \in \mathbb{Z}.$$
$$y = y_1 - \frac{a}{d}s$$

Then, $\quad 0 \le x_1,\ x_1 + \frac{m}{d},\ x_1 + \frac{m}{d}\cdot 2,\ \ldots,\ x_1\frac{m}{d}\cdot(d-1) < m$

and these are exactly the solutions to $ax \equiv b \pmod{m}$. $\square$

We now know exactly how many solutions to expect — How do we find them?

Ex Solve each of the following.

① $\overset{a}{4}x \equiv \overset{b}{2} \pmod{\overset{m}{12}}$

$(a,m) = (4,12) = 4$. $4 \nmid 2 \Rightarrow$ $\boxed{\text{No solutions}}$

② $5x \equiv 2 \pmod{12}$

$(5,12) = 1 \Rightarrow$ 1 solution.

Algebraic Approach

manipulate then cancel

$$
\begin{aligned}
5x \equiv 2 &\Rightarrow 5x \equiv 2 + 12 + 12 + 12 + \cdots \pmod{12} \\
&\Rightarrow 5x \equiv 2 + 48 \pmod{12} \\
&\Rightarrow 5x \equiv 50 \pmod{12}
\end{aligned}
$$

5 is cancellable mod 12, b/c $(5,12)=1$

$$\Rightarrow \boxed{x \equiv 10} \pmod{12}$$

Table Approach (only if modulus is small)

x	0	1	2	3	4	5	6	7	8	9	10
$5x$	0	5	10	15 ≡ 3	20 ≡ 8	25 ≡ 1	30 ≡ 6	35 ≡ 11	40 ≡ 4	45 ≡ 9	50 ≡ 2 ✓

$\boxed{x \equiv 10} \pmod{12}$

③ $9x \equiv 6 \pmod{12}$

$(9,12) = 3$, $3 \mid 6 \Rightarrow$ 3 solutions

Algebraic Approach

* manipulate and cancel

$9x \equiv 6 \pmod{12}$ ← $(9,12) \neq 1$ so can't cancel :(

* use Thm 5 - Sect. 4

(a) Solve the reduced congruence

$$3x \equiv 2 \pmod 4$$

$$3x \equiv 2 \pmod 4 \iff 3x \equiv 6 \pmod 4$$
$$\iff x \equiv 2 \pmod 4$$

(b) "Lift" solutions

- we found

$$9x \equiv 6 \pmod{12} \implies x \equiv 2 \pmod 4$$

- Want all residues mod 12 cong. to 2 mod 4

$2 \equiv 2 \bmod 4$
$6 \equiv 2 \bmod 4$
$10 \equiv 2 \bmod 4$

Table Approach (only if the modulus is small)

x	0	1	2	3	4	5	6	7	8	9	10	11
$9x$	0	9	18	27	36	45	54	63	72	9	6	3
			$\equiv$ 6	$\equiv$ 3	$\equiv$ 0	$\equiv$ 9	$\equiv$ 6	$\equiv$ 3	$\equiv$ 0			

repeat repeat

$\boxed{x \equiv 2, 6, 10}$

Another Example...

$\underline{\text{Ex}}$ Solve $12x \equiv 20 \pmod{28}$

① Find # of sol. : $(12,28)=4$ AND $4 \mid 20$ so 4 solutions

② Solve

$12x \equiv 20 \pmod{28} \xrightarrow{\text{reduce}} 3x \equiv 5 \pmod 7$

$3x \equiv 12 \pmod 7$ 3 is cancellable mod 7

$x \equiv 4 \pmod 7$

back to 28

want All $x \pmod{28}$
such that $x \equiv 4 \pmod 7$

$4 \equiv 4+7 = 11$
$\equiv 4+14 = 18$
$\equiv 4+21 = 25$

ANSWER: $\boxed{x \equiv 4, 11, 18, 25 \pmod{28}}$

Systems of congruences

$\underline{\text{Ex}}$ Solve $x+2y \equiv 4 \pmod{11}$, $3x+y \equiv -1 \pmod{11}$

add

$x+2y \equiv 4 \pmod{11}$
$-2\cdot(3x+y \equiv -1)$
$-6x-2y \equiv 2$

$-5x \equiv 6 \pmod{11}$ cancellable
$-5x \equiv 6 \equiv -5 \Rightarrow \boxed{x \equiv 1}$

$1+2y \equiv_{11} 4$
$2y \equiv_{11} 3$
$2y \equiv_{11} 14$
$\boxed{y \equiv 7}$

Systems of congruences with different moduli

Ever notice that 48, 49, 50 are each divisible by a square... here's a related problem...

16 49 25

$\underline{\text{Ex}}$ Find n such that $3^2 \mid n,\ 4^2 \mid n+1,\ 5^2 \mid n+2$

want to solve

$$\left.\begin{aligned} &① \quad n \equiv 0 \mod 9 \\ &② \quad n+1 \equiv 0 \mod 16 \\ &③ \quad n+2 \equiv 0 \mod 25 \end{aligned}\right\} \text{system of cong.}$$

① $n \equiv 0 \mod 9 \implies \boxed{n = 9r}$ for $r \in \mathbb{Z}$

9 (and 3) are cancellable mod 16

② $n+1 \equiv 0 \mod 16 \implies 9r + 1 \equiv 0 \pmod{16}$

$\implies 9r \equiv -1 \pmod{16}$

$\equiv 15 \equiv 31 \equiv 47 \equiv 63$

$\implies r \equiv 7 \pmod{16}$

$\implies r = 7 + 16s$

$\implies n = 9(7 + 16s)$

$\boxed{n = 63 + 144s}$

③ $n + 2 \equiv 0 \pmod{25} \implies 65 + 144s \equiv 0 \pmod{25}$

$\implies 15 + 19s \equiv 0$

$19s \equiv -15$

$-6s \equiv 10 \equiv 35 \equiv 60$

$s \equiv -10 \equiv 15 \pmod{25}$

$\implies s = 15 + 25t$

$n = 63 + 144(15 + 25t)$

$\boxed{n = 2223 + 3600t}$

Any t works — $t = 0$

$n \equiv 2223 \pmod{\underline{9 \cdot 16 \cdot 25}}$

product of moduli

$\boxed{2223,\ 2224,\ 2225}$

$3^2 \cdot 13 \cdot 19$, $4^2 \cdot 139$, $5^2 \cdot 89$

This process often works...

Thm 2 (Chinese Remainder Theorem)

Consider the system of congruences:

$$n \equiv a_1 \pmod{m_1}$$
$$n \equiv a_2 \pmod{m_2}$$
$$\vdots$$
$$n \equiv a_k \pmod{m_k}$$

If $(m_i, m_j) = 1$ for all $i \neq j$, then the system has a unique solution modulo $m_1 \cdot m_2 \cdot \dots \cdot m_k$.

! Even if the moduli are not pairwise relatively prime, the system may still have solutions.

Ex Find the smallest odd n, $n > 3$, s.t. $3 \mid n$, $5 \mid n+2$, and $7 \mid n+4$.

Need to solve the system:

$$\begin{aligned} n &\equiv 0 \pmod 3 \\ n+2 &\equiv 0 \pmod 5 \\ n+4 &\equiv 0 \pmod 7 \\ n &\equiv 1 \pmod 2 \end{aligned} \iff \begin{aligned} n &\equiv 0 \pmod 3 \\ n &\equiv -2 \pmod 5 \\ n &\equiv -4 \pmod 7 \\ n &\equiv 1 \pmod 2 \end{aligned}$$

moduli are rel. prime so we are guaranteed to have a sol. — now we need to find it — HW!

Using the Euclidean Alg. to solve $ax \equiv b$

Ex Solve $23x \equiv 12 \pmod{97}$

but we won't explicitly use this

- $\gcd(23, 97) = 1$ (so 23 is cancellable mod 97)
- use Euclidean Alg. backwards to find a solution to

$$23x_0 + 97y_0 = 1$$

(do side work...) we find that

$$23 \cdot 38 + 97(-9) = 1$$

- Thus, $\boxed{23 \cdot 38 \equiv 1} \pmod{97}$

behaves like 23^{-1}

- Now,

$$23x \equiv 12 \pmod{97}$$

$$\Longrightarrow 38 \cdot \cancel{23}^{\,1} \cdot x \equiv 38 \cdot 12 \pmod{97}$$

$$\Longrightarrow x \equiv 456 \pmod{97}$$

$$\Longrightarrow \boxed{x \equiv 68} \pmod{97}$$

$$97 \overline{)456}^{\,4} \quad \vdots \quad 68$$