Number Theory Section Summary: 4.4
Linear Congruences

1. Summary

Recall that a **congruence** is an equation of the form $P(x) \equiv 0 (\text{mod n})$; a **linear congruence** should be that equation with $P(x) = ax - b -$ and it is!

$$ax - b \equiv 0 (\text{mod n}) \iff ax \equiv b (\text{mod n})$$

which means that $ax - b = ny$ for some $y \in \mathbf{Z}$; rewriting, we have that

$$ax - ny = b$$

to be solved in integers – that is, a Diophantine equation!

Now the Diophantine equation could have an infinite number of solutions, but since we're working modulo n, we're only interested in solutions distinct mod n.

2. Definitions

linear congruence a congruence in which $P(x)$ is of the form $P(x) = ax - b$.

3. Theorems

Theorem 4.7: The linear congruence $ax \equiv b (\text{mod n})$ has a solution if and only if $d|b$, where $d = \gcd(a, n)$. If $d|b$, then the linear congruence has d mutually incongruent solutions modulo n.

Example: #1bdf, p. 82 Solve the following linear congruences:

- $5x \equiv 2 (\text{mod } 26)$

- $$36x \equiv 8 (\text{mod } 102)$$
- $$140x \equiv 133 (\text{mod } 301)$$

[Hint: $\gcd(140, 301) = 7$]

Corollary: If $\gcd(a, n) = 1$, then the inear congruence $ax \equiv b (\text{mod n})$ has a unique solution modulo n.

Theorem 4.8 (The Chinese Remainder Theorem): Let $n_1, n_2, \ldots, n_r$ be positive integers such that $\gcd(n_i, n_j) = 1$ for $i \neq j$. Then the system of linear congruences

$$\begin{aligned} x &\equiv a_1 (\text{mod } n_1) \\ x &\equiv a_2 (\text{mod } n_2) \\ &\vdots \\ x &\equiv a_r (\text{mod } n_r) \end{aligned}$$

has a simultaneous solution which is unique modulo $N = n_1 n_2 \cdots n_r$.

The unique solution is of the form

$$x = a_1 N_1 x_1 + \ldots + a_r N_r x_r$$

where $N_k = \frac{N}{n_k}$ and x_k is the unique solution to the linear congruence $N_k x \equiv 1 (\text{mod } n_k)$.

Theorem 4.9: The system of linear congruences

$$\begin{aligned} ax + by &\equiv r (\text{mod n}) \\ cx + dy &\equiv s (\text{mod n}) \end{aligned}$$

has a unique solution whenever $\gcd(ad - bc, n) = 1$.

4. Properties/Tricks/Hints/Etc.

For those of you with linear algebra backgrounds, you'll recognize $ad - bc$ in the linear system of Theorem 4.9 as the determinant.

#4a, p82

① $x \equiv 1 (\text{mod } 3)$

② $x \equiv 2 (\text{mod } 5)$

③ $x \equiv 3 (\text{mod } 7)$

① $\Rightarrow$ $x = 1 + 3k$; feed into ②:

② $\Rightarrow$ $1 + 3k \equiv 2 \pmod 5$

$3k \equiv 1 \pmod 5$

$2 \cdot 3k \equiv 2 \pmod 5$

$6k \equiv 2 \pmod 5 \Rightarrow k \equiv 2 \pmod 5$

$k = 2 + 5l$

$x = 1 + 3(2 + 5l)$

$= 7 + 15l$; feed into ③

③ $\Rightarrow 7 + 15l \equiv 3 \pmod 7$

$15l \equiv 3 \pmod 7$

$l \equiv 3 \pmod 7$

$\therefore \quad l = 3 + 7m$

$\therefore x = 7 + 15(3 + 7m)$

$= 52 + 105m$

Check your work i feed x back into ①, ②, & ③.

Using the Chinese Remainder Theorem:

$x \equiv 1 \pmod 3$ $\quad a_1 = 1$ $\quad n_1 = 3$

$x \equiv 2 \pmod 5$ $\quad a_2 = 2$ $\quad n_2 = 5$

$x \equiv 3 \pmod 7$ $\quad a_3 = 3$ $\quad n_3 = 7$

$N_1 = 5 \cdot 7 = 35$

$N_2 = 3 \cdot 7 = 21$

$N_3 = 3 \cdot 5 = 15$

$N = 105$

$$\bar{x} \equiv 1 \cdot 35 \cdot x_1 + 2 \cdot 21 \cdot x_2 + 3 \cdot 15 \cdot x_3 \pmod{N}$$

x_k solutions of $N_k x \equiv 1 \pmod{n_k}$

① $35 \cdot x_1 \equiv 1 \pmod 3 \Rightarrow x_1 \equiv 2 \pmod 3$

② $21 \cdot x_2 \equiv 1 \pmod 5 \Rightarrow x_2 \equiv 1 \pmod 5$

③ $15 \cdot x_3 \equiv 1 \pmod 7 \Rightarrow x_3 \equiv 1 \pmod 7$

$\bar{x} \equiv 70 + 42 + 45 \pmod{105}$

$\bar{x} \equiv 157 \pmod{105}$

$\equiv 52 \pmod{105}$

? (hint) - x # of eggs

① $x \equiv 1 \pmod 2$

② $x \equiv 2 \pmod 3$

③ $x \equiv 3 \pmod 4$ $\Leftrightarrow$ $x \equiv 1 \pmod 2$

④ $x \equiv 4 \pmod 5$

⑤ $x \equiv 5 \pmod 6$

⑥ $x \equiv 0 \pmod 7$

③ ⇒ ①

$x = 3 + 4k$

$= 3 + 2(2k)$

$= 1 + 2(2k+1)$

---

⑤ ⇒ ②

$x = 5 + 6k = 5 + 3 \cdot (2k) = 2 + 3(2k+1)$

$x = 5 + 2(3k) = 1 + 2(3k+2)$ ⑤ ⇒ ①

Show that

② $x \equiv 1 \pmod 2$
③ $x \equiv 2 \pmod 3$
$\Rightarrow x \equiv 5 \pmod 6$

The grungy way....

② $\Rightarrow x = 1 + 2k$; feed into ③

$1 + 2k \equiv 2 \pmod 3$

$2k \equiv 1 \pmod 3$

$-k \equiv 1 \pmod 3$

$k \equiv 2 \pmod 3$

$\therefore k = 2 + 3j$; plug into x, ←

$x = 1 + 2(2 + 3j) = 5 + 6j$

$\therefore x \equiv 5 \pmod 6$

#10 p82

$x \equiv 3 \pmod{17}$

$x \equiv 10 \pmod{16}$

$x \equiv 0 \pmod{15}$

$$x = 3930 + 4080k$$
$$\equiv 3930 \pmod{4080}$$

206, p 83

① $7x + 3y \equiv 6 \pmod{11}$

② $4x + 2y \equiv 9 \pmod{11}$

$\gcd(7 \cdot 2 - 3 \cdot 4, 11)$
$= 1$ ✓

a① $- b$② $\Rightarrow$

$$2x \equiv -15 \pmod{11}$$
$$\equiv 7 \pmod{11}$$
$$10x \equiv 35 \pmod{11}$$
$$-x \equiv 2 \pmod{11}$$
$$x \equiv 9 \pmod{11}$$

a② $- c$① $\Rightarrow$

$$2y \equiv 6 \pmod{11}$$
$$5 \cdot 2y \equiv 5 \cdot 6 \pmod{11}$$
$$10y \equiv 30 \pmod{11}$$
$$-y \equiv -3 \pmod{11}$$
$$y \equiv 3 \pmod{11}$$

$y \equiv 3 \pmod{11}$

Check:

$x = 9$, $y = 3$ a solution to the system?

$$\left.\begin{aligned} 7x + 3y &\equiv 6 \pmod{11} \\ 4x + 2y &\equiv 9 \pmod{11} \end{aligned}\right\} \Rightarrow \begin{aligned} 72 &\equiv 6 \pmod{11} \\ 42 &\equiv 9 \pmod{11} \end{aligned}$$

#19

$$3x + 4y \equiv 5 \pmod{8}$$

$$3x \equiv 5 - 4y \pmod{8}$$

Consider

$$3z \equiv 1 \pmod{8} \quad (*)$$

$$\boxed{z \equiv 3 \pmod{8}}$$

$y = 0, 1, 2, \ldots, 7$

$y = 0$: $3x \equiv 5 \pmod{8}$

Multiply (*) by 5:

$5 \cdot 3z \equiv 5 \pmod 8$

$3(5z) \equiv 5 \pmod 8$

Solution : $x \equiv 5z \equiv 15 \equiv 7 \pmod 8$