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 $y \in \mathbb{Z}$; 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.

$ax \equiv b \pmod n \iff ax - b = ny \quad \exists y \in \mathbb{Z}$

$\iff ax - ny = b$

linear combinations of a & n look like multiples of the gcd : therefore, for a solution to exist $b = md$ where $d = \gcd(a, n)$.

If $\exists$ a solution, i.e. $b = md$ for $m \in \mathbb{Z}$, say $\langle x_0, y_0 \rangle$

Then all solns are given by

$$\langle x_0 + \tfrac{n}{d}t \,,\, y_0 + \tfrac{a}{d}t \rangle$$

Consider $t \in \{0, 1, \ldots, d-1\}$

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

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

- $5x \equiv 2 \pmod{26} \equiv -50 \pmod{26}$

  $ax \equiv b \pmod{n}$

  ① $\gcd(a, n) = 1$ ∴ ∃! soln.

  ② $5 \cdot 5x \equiv 5 \cdot 2 \pmod{26}$

  $25x \equiv 10 \pmod{26}$

  $25 = 26 - 1$

  $-1x \equiv 10 \pmod{26}$

  $x \equiv -10 \pmod{26}$

  $\boxed{x \equiv 16 \pmod{26}}$

  $x \equiv -10 \pmod{26}$

- $36x \equiv 8 \pmod{102}$

  ① $\gcd(36, 102) = 6$

  ② Is there a soln? $6 \nmid 8 \Rightarrow$ no soln.

$$140x \equiv 133 \pmod{301}$$

① [Hint: $\gcd(140, 301) = 7$]

② 7 7 solns ($7 \mid 133 \Rightarrow$ 7 a soln; $d = 7 \Rightarrow$ 7 7 distinct (incongruent) solns)

③ Find 'em! Divide through by 7:

$20x \equiv 19 \pmod{43}$ has a unique soln, as $\gcd(20, 43) = 1$. Find it, or hack on multiples of 43.

$\Rightarrow \quad 60x \equiv 57 \pmod{43}$

$\equiv 100 \pmod{43}$

$\therefore \quad 6x \equiv 10 \pmod{43}$

$\Rightarrow \quad 42x \equiv 70 \pmod{43}$

$\therefore \quad -1x \equiv 70 \pmod{43}$

$x \equiv -70 \pmod{43}$

$\equiv -27 \pmod{43}$

$\equiv 16 \pmod{43}$

That's 1 soln: the rest look like

$x = 16 + 43t \quad$ where $t \in \{0, \ldots, 6\}$

7 distinct solns mod 301.

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

$$\begin{aligned} x &\equiv a_1 \pmod{n_1} \\ x &\equiv a_2 \pmod{n_2} \\ &\vdots \\ x &\equiv a_r \pmod{n_r} \end{aligned}$$

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 $N_k x \equiv 1 \pmod{n_k}$. $\quad \gcd(N_k, n_k) = 1$

Example: Find x such that x hours from midnight will be 6:00 AM, and such that x days from Sunday will be Thursday.

$$\begin{aligned} x &\equiv 6 \pmod{24} \\ x &\equiv 4 \pmod{7} \end{aligned}$$

$a_1 = 6 \quad n_1 = 24 \quad N_1 = 7 \quad x_1 = 7$

$a_2 = 4 \quad n_2 = 7 \quad N_2 = 24 \quad x_2 = 5$

$N = 24 \cdot 7 = 168$

solve $\begin{cases} 7x_1 \equiv 1 \pmod{24} \\ 24x_2 \equiv 1 \pmod{7} \end{cases}$

$$\bar{x} = 6 \cdot 7 \cdot 7 + 4 \cdot 24 \cdot 5 = 774 \equiv 102 \pmod{168}$$

$7x_1 \equiv 1 \pmod{24} \Rightarrow 7 \cdot 7x_1 \equiv 7 \pmod{24}$

$\Rightarrow 49x_1 \equiv 7 \pmod{24}$

$\Rightarrow x_1 \equiv 7 \pmod{24}$

$24x_2 \equiv 1 \pmod{7} \Rightarrow 48x_2 \equiv 2 \pmod{7}$

$\Rightarrow -1 x_2 \equiv 2 \pmod{7}$

$\Rightarrow x_2 \equiv -2 \pmod{7} \equiv 5 \pmod{7}$

Check: $102 \equiv 6 \pmod{24}$

$102 \equiv 4 \pmod{7}$ ✓

Theorem 4.9: The system of linear congruences

$$ax + by \equiv r \pmod{n}$$
$$cx + dy \equiv s \pmod{n}$$

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

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

$adx + bdy \equiv dr \pmod{n}$
$-\ bcx + bdy \equiv bs \pmod{n}$
$(ad-bc)x \equiv dr - bs \pmod{n}$
so there's a unique soln.

Similarly for y:
$cax + bcy \equiv cr \pmod{n}$
$cax + ady \equiv as \pmod{n}$
$\Rightarrow (ad-bc)y \equiv as - cr \pmod{n}$

Solve instead
$(ad-bc)z \equiv 1 \pmod{n}$
for solution z,
$x \equiv z(dr-bs) \pmod{n}$
$y \equiv z(as-cr) \pmod{n}$

Example #20, p. 83: Find the solutions of each:

- (a)

$$5x + 3y \equiv 1 \pmod{7}$$
$$3x + 2y \equiv 4 \pmod{7}$$

① $ad-bc = 5\cdot 2 - 3\cdot 3 = 1$
$\gcd(1,7) = 1 \Rightarrow$ 1! soln.

② Solve $(ad-bc)z \equiv 1 \pmod{7}$
$z \equiv 1 \pmod{7}$
$x \equiv 2\cdot 1 - 3\cdot 4 \equiv -10 \equiv 4 \pmod{7}$
$y \equiv 5\cdot 4 - 3\cdot 1 \equiv 17 \equiv 3 \pmod{7}$

③ Check: $5\cdot 4 + 3\cdot 3 = 29 \equiv 1 \pmod{7}$ ✓
$3\cdot 4 + 2\cdot 3 = 18 \equiv 4 \pmod{7}$

- (b)

$$7x + 3y \equiv 6 \pmod{11}$$
$$4x + 2y \equiv 9 \pmod{11}$$

① $\gcd(ad-bc, n) = ?$ $\gcd(2, 11) = 1$
$ad - bc = 2 \Rightarrow$ 1! soln

② $2\cdot z \equiv 1 \pmod{11} \equiv 12 \pmod{11}$
$\therefore z \equiv 6 \pmod{11}$

③ $x \equiv 6\cdot(-15) = -90 \equiv 9 \pmod{11}$
$y \equiv 6\cdot(39) \equiv 3 \pmod{11}$
$6\cdot(33+6) = 36 \equiv 3 \pmod{11}$

- (c)

$$11x + 5y \equiv 7 \pmod{20}$$
$$6x + 3y \equiv 8 \pmod{20}$$

#8 When eggs are removed 2,3,4,5,6 at a time the remain 1 2 3 4 5 eggs.

① $x \equiv 1 \pmod 2$

② $x \equiv 2 \pmod 3$

③ $x \equiv 3 \pmod 4$

④ $x \equiv 4 \pmod 5$

⑤ $x \equiv 5 \pmod 6$

⑥ $x \equiv 0 \pmod 7$

③ or ⑤ $\Rightarrow$ ①

③ + ② $\Rightarrow$ ⑤

$x = 1 + 6k$? $\Rightarrow 3(2k)+1$

$x = 3 + 6k$? $\Rightarrow 3 \mid x$

contradict ②

Now we can invoke the Chinese remainder theorem.

$x \equiv 2 \pmod 3 \Rightarrow x = 2 + 3k$

$2 + 3k \equiv 3 \pmod 4$

$3k \equiv 1 \pmod 4 \equiv 9 \pmod 4 \Rightarrow k \equiv 3 \pmod 4$

$k = 3 + 4l$

$x = 2 + 3(3 + 4l) = 11 + 12l$

$11 + 12l \equiv 4 \pmod 5$

$12l \equiv -7 \pmod 5$

$12l \equiv -12 \pmod 5 \quad \Rightarrow \quad l \equiv -1 \bmod 5 \equiv 4 \pmod 5$

$\therefore l = 4 + 5m$

$x = 11 + 12(4 + 5m) = 59 + 60m$

$59 + 60m \equiv 0 \pmod 7$

$60m \equiv 4 \pmod 7$

$\equiv 60 \pmod 7 \quad \therefore m \equiv 1 \pmod 7$

$m = 1 + 7n$

$x = 59 + 60(1 + 7n)$

$= 119 + 420n$

$x \equiv 119 \pmod{420}$

$\uparrow$ 3.4.5.7

$x = 119 + 420n$

$119 + 420n \equiv 1 \pmod 2$

$420n \equiv -118 \pmod 2$

$\equiv 0 \pmod 2$

$\Rightarrow$ any value of n makes tri. 1 true — no new constraint

$119 + 420n \equiv 5 \pmod 6$

$420n \equiv 0 \pmod 6$

$\Rightarrow$ no new constraint.

$\therefore$ 119 eggs