Solving Congruences

Wednesday, April 8, 2026 11:15 AM

Missing:
700#4,
800#3, 25
+B#729, 16, 13, 27, 812 (Longest chain)
+B#705, 706, 708
+B#807, 813, 810, 811, 820

Recall: Euclidean Algorithm

1] Extended Euclidean Algorithm (EEA)

Thm: if $a, b \in \mathbb{Z}^+$, then there exist unique $s, t \in \mathbb{Z}$ such that $\gcd(a,b) = s \cdot a + t \cdot b$

Thus, $\gcd(a,b)$ can be expressed as a linear combination of a and b.

2] e.g. Write the $\gcd(156, 69)$ as a linear combination of 156 and 69.

$\gcd = 3 = \frac{?}{s} \cdot 156 + \frac{?}{t} \cdot 69$

Soln.

$156 = \underline{2} \cdot 69 + 18$ ——①

$69 = \underline{3} \cdot 18 + 15$ ——②

$18 = \underline{1} \cdot 15 + 3$ ——③

$15 = \underline{5} \cdot 3 + 0$

from ③:

$3 = 18 - 1 \cdot 15$

$= 18 - 1 \cdot (69 - 3 \cdot 18)$ by ②

$= -1 \cdot 69 + 4 \cdot 18$

$= -1 \cdot 69 + 4 (156 - 2 \cdot 69)$

$= +4 \cdot 156 - 9 \cdot 69$

$\therefore s = 4, \ t = -9$

3] Lemma: if $a, b, c \in \mathbb{Z}^+$, with $\gcd(a,b) = 1$ and $a \mid bc$ then $a \mid c$

e.g. $15 \mid (14 \cdot 30) \implies 15 \mid 30$

$15 \mid (12 \cdot 20) \not\implies 15 \mid 20$ since $\gcd(15, 12) \neq 1$

4] Lemma: if prime and $p \mid a_1 \cdot a_2 \cdot a_3 \cdots a_n$; $a_i \in \mathbb{Z}$,
then $p \mid a_i$ for some a_i

5] Linear Congruences (§4.4)

To solve for x in:

$$ax \equiv b \pmod{m}$$

e.g.

$$5x \equiv 6 \pmod{11}$$

6] Def^n. the inverse of a modulo m is a^{-1} (or $\bar{a}$)

classnote notation

textbook and exam notation

s.t.

$$a \cdot a^{-1} \equiv 1 \pmod{m}$$

e.g.

$$5^{-1} \equiv 9 \pmod{11}$$

7] Exer: Find the inverse of $a = 1, 2, \ldots, 10 \pmod{11}$

a	1	2	3	4	5	6	7	8	9	10
$a^{-1} = \bar{a}$	1	6	4	3	9	2	8	7	5	10

$(-1)(-1)$

8] Exer: Find the inverse of $a = 1, 2, \ldots, 9 \pmod{10}$

a	0	1	2	3	4	5	6	7	8	9
$\bar{a}$	—	1	—	7	—	—	—	3	—	9

+B#807, 813) +B#5, 6

9] Thrm: a has an inverse modulo m iff $\gcd(a, m) = 1$ and a^{-1} is unique in $\mathbb{Z}_m$

proof: (How to find a^{-1})

Since $\gcd(a, m) = 1$,

We can write $1 = s \cdot a + t \cdot m$ by EEA.

$\Rightarrow 1 \equiv s \cdot a + t \cdot m \pmod{m}$

$\Rightarrow 1 \equiv s \cdot a + 0 \pmod{m}$

$\therefore a^{-1} \equiv s$

10] e.g.

F14 Find $5^{-1} \pmod{22}$

$22 = 4 \cdot 5 + 2$

$5 = 2 \cdot 2 + 1$

$1 = 5 - 2 \cdot 2$

$= 5 - 2(22 - 4 \cdot 5)$

$= -2 \cdot 22 + 9 \cdot 5$

$\therefore 5^{-1} = 9$

Verify: $5 \cdot 9 = 45 \equiv 1 \pmod{22}$

F13 Find $3^{-1} \pmod{7}$

Soln. $7 = 2 \cdot 3 + 1$

$3 = 3 \cdot 1 + 0$ ← gcd

$\Rightarrow 1 = 7 - 2 \cdot 3$

$\therefore 5 = -2 \Rightarrow 3^{-1} = -2 \equiv 5 \pmod{7}$

Verify:

11) How to solve a linear congruence

$$ax \equiv b \pmod{m}$$

① find a^{-1} if $\gcd(a, m) = 1$

② multiply both sides by a^{-1}

$$\Rightarrow x \equiv b \cdot a^{-1} \pmod{m}$$

12) e.g.

$$5 \cdot x \equiv 6 \pmod{11}$$

$$\Rightarrow x \equiv 6 \cdot 5^{-1}$$

$$\equiv 6 \cdot 9 \equiv 54 \equiv 10 \pmod{11}$$

Verify: $5 \cdot (10) \equiv 50 \equiv 6 \pmod{11}$

13) Note. (about [11])

What if $\gcd(a, m) = d \neq 1$?

$ax \equiv b \pmod{m}$

- $d \nmid b \Rightarrow$ no solution
- $d \mid b \Rightarrow$ simplify $\Rightarrow$ we have d solutions

e.g.

$$15x \equiv 18 \pmod{33}$$

Simplify $\Rightarrow$ $5x \equiv 6 \pmod{11}$

$$\Rightarrow x \equiv 6 \cdot 5^{-1} \equiv 6 \cdot 9 \equiv 10 \pmod{11}$$

In mod 33, we have $x = 10, 21, 32$; $(x = 10 + 11k)$

14] Exer: Divisibility

by ③ : Add the digits

e.g. ① 2784

$\xrightarrow{+}$ 21 $\Longrightarrow$ $2784 \equiv 0 \pmod 3$

② 2786

$\xrightarrow{+}$ $23 \equiv 2 \pmod 3$

by ⑪ : _____

e.g. $2789 \equiv 6 \pmod{11}$

by ⑦

$2789 \equiv 3$

+B810
+B708

by ⑥ $2789 \equiv 5$ +B811

by ⑨ $2789 \equiv 8$ +B820

15] Divisibility Rules: when dividing by n ?

by 3: Add the digits (mod 3)

$2789 = 2 \times 10^3 + 7 \times 10^2 + 8 \times 10^1 + 9$

$$2789 = 2\times10^3 + 7\times10^2 + 8\times10 + 9$$
$$\equiv 2(1^3) + 7(1^2) + 8(1) + 9 \pmod 3$$
$$\equiv 2 + 7 + 8 + 9$$
$$\equiv 26$$
$$\equiv 2+6 \equiv 8 \equiv 2 \pmod 3$$

by 9 : Add the digits (cast out 9's)

$$2789 \equiv 8 \pmod 9$$

by 6 : check if divisible by 3 and even

by 11 : Alternating +/− from Right to Left

$$2789 = 2\times10^3 + 7\times10^2 + 8\times10 + 9$$
$$\equiv 2(-1)^3 + 7(-1)^2 + 8(-1) + 9 \pmod{11}$$
(− + − +)

from R to L $= -2 + 7 - 8 + 9$

Alternate +/−

$$\overset{-}{3}\,7\,8\,8\,7\,\overset{+}{4} \equiv 1$$

$$1\,5\,7\,2\,2\,7\,5\,5 \equiv 4$$