Fifth Exercise Session: 27/4

Themes: Number theory, Group theory (optional)

Relevant Chapters: Vol.1: 3; Suppl4.pdf; Vol. 2: 2 (optional)

1. Compute the inverse of 37 in $\mathbb{Z}_{103}^{\times}$.

2. Determine the general solution of the system

$$2x \equiv 1 \pmod 9, \quad 3x \equiv 2 \pmod{10}, \quad 4x \equiv 3 \pmod{11}.$$

3. For which $b \in \mathbb{Z}$ does the congruence $36x \equiv b \pmod{100}$ have a solution ? Find the general solution for $b = 68$.

4. (i) Explain the "digit sum trick" for testing whether a number is divisible by 9 (resp. 3).
(ii) Determine, with proof, a similar trick for testing divisibility by 11.

Solutions

1. Note that the inverse exists, since 103 and 37 are both primes and hence we know in advance that $\mathrm{GCD}(103,\ 37) = 1$. Euclid forwards:

$$\begin{aligned} 103 &= 2 \cdot 37 + 29, \\ 37 &= 1 \cdot 29 + 8, \\ 29 &= 3 \cdot 8 + 5, \\ 8 &= 1 \cdot 5 + 3, \\ 5 &= 1 \cdot 3 + 2, \\ 3 &= 1 \cdot 2 + 1. \end{aligned}$$

Then backwards:

$$\begin{aligned} 1 &= 3 - 2 \\ &= 3 - (5 - 3) \\ &= 2 \cdot 3 - 5 \\ &= 2(8 - 5) - 5 \\ &= 2 \cdot 8 - 3 \cdot 5 \\ &= 2 \cdot 8 - 3(29 - 3 \cdot 8) \\ &= 11 \cdot 8 - 3 \cdot 29 \\ &= 11(37 - 29) - 3 \cdot 29 \\ &= 11 \cdot 37 - 14 \cdot 29 \\ &= 11 \cdot 37 - 14(103 - 2 \cdot 37) \end{aligned}$$

$$\Rightarrow \quad 1 = (-14) \cdot 103 + 39 \cdot 37.$$

Reading this modulo 103, we have

$$1 \equiv 39 \cdot 37 \pmod{103}$$

and hence $37^{-1} \equiv 39 \pmod{103}$.

2. First some editing:

$$\begin{aligned} 2x \equiv 1 \pmod 9 &\Rightarrow x \equiv 2^{-1} \cdot 1 \equiv 5 \cdot 1 \equiv 5 \pmod 9, \\ 3x \equiv 2 \pmod{10} &\Rightarrow x \equiv 3^{-1} \cdot 2 \equiv 7 \cdot 2 \equiv 4 \pmod{10}, \\ 4x \equiv 3 \pmod{11} &\Rightarrow x \equiv 4^{-1} \cdot 3 \equiv 3 \cdot 3 \equiv -2 \pmod{11}. \end{aligned}$$

Thus, by eq. (11.3) in the lecture notes, the general solution is

$$x \equiv 5 \cdot b_1 \cdot 10 \cdot 11 + 4 \cdot b_2 \cdot 9 \cdot 11 - 2 \cdot b_3 \cdot 9 \cdot 10 \pmod{9 \cdot 10 \cdot 11}, \tag{1}$$

where

$$\begin{aligned} b_1 &\equiv (10 \cdot 11)^{-1} \equiv (1 \cdot 2)^{-1} \equiv 2^{-1} \equiv 5 \pmod 9, \\ b_2 &\equiv (9 \cdot 11)^{-1} \equiv ((-1) \cdot 1)^{-1} \equiv (-1)^{-1} \equiv -1 \pmod{10}, \\ b_3 &\equiv (9 \cdot 10)^{-1} \equiv ((-1) \cdot (-2))^{-1} \equiv 2^{-1} \equiv 6 \pmod{11}. \end{aligned}$$

We choose $b_1 = 5$, $b_2 = -1$, $b_3 = 6$ and insert into (1) to get

$$\begin{aligned} x &\equiv 5 \cdot 5 \cdot 10 \cdot 11 + 4 \cdot (-1) \cdot 9 \cdot 11 - 2 \cdot 6 \cdot 9 \cdot 10 \\ &\equiv 2750 - 396 - 1080 \equiv 1274 \equiv 284 \pmod{990}. \end{aligned}$$

ANSWER: $x \equiv 284 \pmod{990}$.
SANITY CHECK: Check that $x = 284$ satisfies the original three congruences by direct calculation:
$284 - 5 = 279 = 9 \cdot 31$, ok
$284 - 4 = 280 = 10 \cdot 28$, ok
$284 - (-2) = 286 = 11 \cdot 26$, ok !

3. Proposition. *Let $n \in \mathbb{Z}_+$ and $a,\, b \in \mathbb{Z}$. Then the congruence*

$$ax \equiv b \ (\mathit{mod}\ n)$$

has a solution if and only if $d \,|\, b$, where $d = \mathit{GCD}(a,\, n)$. In that case, the general solution is given by

$$x \equiv \left(\frac{a}{d}\right)^{-1} \cdot \left(\frac{b}{d}\right) \ \left(\mathit{mod}\ \tfrac{n}{d}\right). \tag{2}$$

PROOF: We have the following equivalences:

$$\begin{aligned} &\exists\, x \in \mathbb{Z} :\ ax \equiv b \pmod{n} \\ &\Leftrightarrow\ \exists\, x \in \mathbb{Z} :\ n \,|\, ax - b \\ &\Leftrightarrow\ \exists\, x,\, y \in \mathbb{Z} :\ ax - b = ny \\ &\Leftrightarrow\ \exists\, x,\, y \in \mathbb{Z} : ax - ny = b. \end{aligned}$$

By Theorem 7.12, such x and y exist if and only if $\mathrm{GCD}(a,\, n)$ divides b, v.s.v. Supposing this is the case, note that

$$\exists\, x,\, y \in \mathbb{Z} :\ ax - ny = b \ \Leftrightarrow\ \exists\, x,\, y \in \mathbb{Z} :\ \left(\frac{a}{d}\right) x - \left(\frac{n}{d}\right) y = \frac{b}{d}.$$

Then running the above sequence of equivalences backwards, this is in turn equivalent to

$$\left(\frac{a}{d}\right) x \equiv \frac{b}{d} \ \left(\mathrm{mod}\ \tfrac{n}{d}\right). \tag{3}$$

Since now $\mathrm{GCD}\left(\frac{a}{d},\, \frac{n}{d}\right) = 1$, $\left(\frac{a}{d}\right)^{-1} \ \left(\mathrm{mod}\ \frac{n}{d}\right)$ exists and thus (3) is equivalent to (2), v.s.v.

Turning to our example, $\mathrm{GCD}(36,\, 100) = 4$. Hence the congruence has a solution if and only if b is a multiple of 4, in which case the general solution is

$$x \equiv 9^{-1} \cdot \left(\frac{b}{4}\right) \equiv 14 \cdot \frac{b}{4} \equiv \frac{7b}{2} \pmod{25}.$$

For $b = 68$, this becomes $x \equiv 238 \equiv 13 \pmod{25}$.

4. Let N be a k-digit number. This means one would write $N = a_{k-1} \ldots a_1 a_0$, where each $a_i \in \{0,\ 1,\ \ldots,\ 9\}$ and $a_{k-1} \neq 0$, and that

$$N = \sum_{i=0}^{k-1} a_i \cdot 10^i.$$

Mod 9: $10 \equiv 1$ so $10^i \equiv 1^i \equiv 1$ for every i. Hence $N \equiv \sum_i a_i \pmod 9$.

Mod 11: $10 \equiv -1$ so $10^i \equiv (-1)^i$ for every i. Hence $N \equiv \sum_i (-1)^i a_i \pmod{11}$.

In words, we have shown that

Every decimal number is congruent to its own digit sum modulo 9

and

Every decimal number is congruent to its own alternating digit sum modulo 11.