Lecture 29

Handout or Document Camera or Class Exercise

Solve the following equations in $\mathbb{Z}_{14}$. Express answers as $[x]$ where $0 \leq x < 14$.

i) $[75] - [x] = [50]$

ii) $[10][x] = [1]$

iii) $[10][x] = [2]$

Hint: Rewrite these using congruences.

Instructor's Comments: Note to "properly" prove these, you would have to prove these as an equality of sets.

Solution:

(i) $[75] - [x] = [50]$ is equivalent to solving $75 - x \equiv 50 \pmod{14}$. Solving here gives $x \equiv 25 \equiv 11 \pmod{14}$.

(ii) $[10][x] = [1]$ is equivalent to solving $10x \equiv 1 \pmod{14}$. Since $\gcd(10, 14) = 2 \nmid 1$, we see by LCT1 that this has no solution.

(iii) $[10][x] = [2]$ is equivalent to solving $10x \equiv 2 \pmod{14}$. Notice that $x = 3$ is a solution and so by LCT1, we see that $x \equiv 3 \pmod{14/\gcd(2, 14)}$ gives a complete solution. This is the same as $x \equiv 3 \pmod{7}$ or $x \equiv 3, 10 \pmod{14}$ or $x = [3], [10]$.

Instructor's Comments: This is the 10 minute mark. The last point that $x \equiv 3 \pmod{7}$ and $x \equiv 3, 10 \pmod{14}$ are equivalent is lost on some students. Remind them that the first meant $x = 3 + 7k$ and that k has two options - being even (which is equivalent to 3 modulo 14) or being odd (which is equivalent to 10 modulo 14). A similar argument can be applied if it were say 7 to 21 etc.

Instructor's Comments: If you want an extra problem with congruences, try Solve $[15][x] + [7] = [12]$ in $\mathbb{Z}_{10}$. Otherwise mention this later.

Inverses

(i) $[-a]$ is the additive inverse of $[a]$, that is, $[a] + [-a] = [0]$.

(ii) If there exists an element $[b] \in \mathbb{Z}_m$ such that $[a][b] = [1] = [b][a]$, we call $[b]$ the multiplicative inverse of $[a]$ and write $[b] = [a]^{-1}$ or $b \equiv a^{-1} \pmod{m}$.

Example: $[5][11] = [1]$ in $\mathbb{Z}_{18}$. Therefore, $[5]^{-1} = [11]$ and $[11]^{-1} = [5]$.

Note: WARNING Multiplicative inverses do not always exist!

Example: $[9][x] = [1]$ in $\mathbb{Z}_{18}$ has no solution. The left hand side is always $[0]$ or $[9]$ for every value of $[x]$. Hence $[9]^{-1}$ does not exist in $\mathbb{Z}_{18}$.

Instructor's Comments: This is the 15 minute mark

Handout or Document Camera or Class Exercise

Find the additive and multiplicative inverses of $[7]$ in $\mathbb{Z}_{11}$. Give your answers in the form $[x]$ where $0 \leq x \leq 10$.

Solution: Additive inverse: $[-7] = [4]$. For the multiplicative inverse, we want to solve

$$[7][x] = [1] \qquad \Leftrightarrow \qquad 7x \equiv 1 \pmod{11}$$

You can solve this by turning this into the LDE $7x + 11y = 1$ and solving that. However, because the numbers are small, guessing and checking is a far more efficient strategy. Notice that

$$7 \cdot 3 \equiv 21 \equiv 10 \equiv -1 \pmod{11}$$

Thus, $7(-3) \equiv 1 \pmod{11}$ and so $[x] = [-3] = [8]$ is the inverse of $[7]$ in $\mathbb{Z}_{11}$.

Instructor's Comments: This is the 25 minute mark

Proposition: Let $a \in \mathbb{Z}$ and $m \in \mathbb{N}$.

(i) $[a]^{-1}$ exists in $\mathbb{Z}_m$ if and only if $\gcd(a, m) = 1$.

(ii) $[a]^{-1}$ is unique if it exists.

Proof:

(i)

$$\begin{array}{lcl} [a]^{-1} \text{ exists} & \Leftrightarrow & [a][x] = [1] \text{ is solvable in } \mathbb{Z}_m \\ & \Leftrightarrow & ax + my = 1 \text{ is a solvable LDE} \\ & \Leftrightarrow & \gcd(a, m) = 1 \text{ GCDOO} \end{array}$$

completing the proof. ■

(ii) Assume $[a]^{-1}$ exists. Suppose there exists a $[b] \in \mathbb{Z}_m$ such that $[a][b] = [1] = [b][a]$. Then

$$\begin{aligned} [a]^{-1}[a][b] &= [a]^{-1}[1] \\ [1][b] &= [a]^{-1} \\ [b] &= [a]^{-1} \end{aligned}$$

Instructor's Comments: This is the 35 minute mark

Exercise: Solve $[15][x] + [7] = [12]$ in $\mathbb{Z}_{10}$.

Instructor's Comments: Solution: This is equivalent to solving

$$15x + 7 \equiv 12 \pmod{10}.$$

Isolating for x gives

$$15x \equiv 5 \pmod{10}.$$

Since $15 \equiv 5 \pmod{10}$, Properties of Congruences states that

$$5x \equiv 5 \pmod{10}.$$

This clearly has the solution $x = 1$. Hence, by Linear Congruence Theorem 1, we have that

$$x \equiv 1 \pmod{\tfrac{10}{\gcd(5,10)}}$$

gives the complete set of solutions. Thus, $x \equiv 1 \pmod{2}$ or $x \equiv 1, 3, 5, 7, 9 \pmod{10}$. Since the original question is framed in terms of congruence classes, our answer should be as well and hence

$$[x] \in \{[1], [3], [5], [7], [9]\}.$$

For extra practice, see if you can phrase this argument using Linear Congruence Theorem 2.

Handout or Document Camera or Class Exercise

Instructor's Comments: This is a good time to introduce the notation TFAE

The following are equivalent [TFAE]

- $a \equiv b \pmod{m}$
- $m \mid (a - b)$
- $\exists k \in \mathbb{Z}, a - b = km$
- $\exists k \in \mathbb{Z}, a = km + b$
- a and b have the same remainder when divided by m
- $[a] = [b]$ in $\mathbb{Z}_m$.

Theorem: [LCT 2] Let $a, c \in \mathbb{Z}$ and let $m \in \mathbb{N}$. Let $\gcd(a, m) = d$. The equation $[a][x] = [c]$ in $\mathbb{Z}_m$ has a solution if and only if $d \mid c$. Moreover, if $[x] = [x_0]$ is one particular solution, then the complete solution is

$$\left\{[x_0], [x_0 + \tfrac{m}{d}], [x_0 + 2\tfrac{m}{d}], \ldots, [x_0 + (d-1)\tfrac{m}{d}]\right\}$$

Instructor's Comments: This is the 40 minute mark

Instructor's Comments: This is the FLT part of the course. I think this proof is fantastic and really creative so I like doing it. One could of course prove FLT using induction and the binomial theorem, which I would say if you have in the course you should do. You can choose to not to the proof or maybe show why it's true for a specific prime but I like actually showing the proof. It's elegant clever and really just awesome. I recommend being brave and showing it. This proof will spill over to the next lecture. Keep shifting content until you reach the square and multiply algorithm which is optional material that you can afford to skip and catch up there.

Theorem: Fermat's Little Theorem (FℓT). If p is a prime number and $p \nmid a$ then $a^{p-1} \equiv 1 \pmod{p}$. Equivalently, $[a^{p-1}] = [1]$ in $\mathbb{Z}_p$.

Example:

(i) $5^6 \equiv 1 \pmod{7}$

(ii) $4^6 \equiv 1 \pmod{7}$

(iii) $39^6 \equiv 1 \pmod{7}$

Note: $p-1$ is in the exponent and not the base. For example, $(5-1)^3 \equiv 4 \pmod{5}$.

Note: $p-1$ is not necessarily the smallest exponent such that $a^k \equiv 1 \pmod{p}$. For example $6^2 \equiv 1 \pmod{7}$.

Lemma: Let $\gcd(a,p) = 1$. Let

$$S := \{a, 2a, ..., (p-1)a\} \qquad T := \{1, 2, ..., p-1\}.$$

Then the elements of S are unique modulo p and for all $s \in S$, there exists a unique element $t \in T$ such that $s \equiv t \pmod{p}$.

Proof: We first show that S contains $p-1$ distinct nonzero elements modulo p.

Let $ka, ma \in S$ with $1 \leq k, m \leq p-1$ integers. Now, if $ka \equiv ma \pmod{p}$, then $p \mid a(k-m)$. Since $\gcd(a,p) = 1$, we see that $p \mid (k-m)$ by Coprimeness and Divisibility. Since

$$-p < 2 - p \leq k - m \leq p - 2 < p$$

and $p \mid (k-m)$, we see that $k - m = 0$, that is, $k = m$. Lastly, if $ka \equiv 0 \pmod{p}$, then $p \mid ka$. By Euclid's Lemma, $p \mid k$, a contradiction since $1 \leq k \leq p-1$ and p is prime, or $p \mid a$ also a contradiction since $\gcd(a,p) = 1$. Thus, S has $p-1$ distinct nonzero elements modulo p.

So if $ka \in S$, then $ka \equiv n \pmod{p}$ for some $1 \leq n \leq p-1$ and this n is unique since if in addition $ka \equiv \ell \pmod{p}$ with $1 \leq \ell \leq p-1$, subtracting the two congruences gives $p \mid (n - \ell)$, a contradiction unless $\ell = n$ since

$$-p < 2 - p \leq \ell - n \leq p - 2 < p.$$

This completes the proof. ■

Proof: (of Fermat's Little Theorem). Using the lemma, valid since $p \nmid a$ holds if and only if $\gcd(a, p) = 1$ (by say GCDPF), we have that by the lemma S and T contain the same elements modulo p and hence their products must be congruent modulo p. Thus,

$$\prod_{x \in S} x \equiv \prod_{y \in T} y \pmod{p}$$
$$\prod_{k=1}^{p-1} ka \equiv \prod_{j=1}^{p-1} j \pmod{p}$$
$$a^{p-1} \prod_{k=1}^{p-1} k \equiv \prod_{j=1}^{p-1} j \pmod{p}$$

Let $Q = \prod_{j=1}^{p-1} j = (1)(2)...(p-1)$. Then

$$Qa^{p-1} \equiv Q \pmod{p}$$

Since $\gcd(Q, p) = 1$ (as Q is a product of numbers less than a prime p), we have that Q^{-1} exists and hence

$$Q^{-1}Qa^{p-1} \equiv Q^{-1}Q \pmod{p}$$

and thus $a^{p-1} \equiv 1 \pmod{p}$ completing the proof . ■

Instructor's Comments: This is the 50 minute mark. It's a bit of an intense proof but really cool.