MATH 2170-19W Problem Set 7

March 29, 2019

Solutions

[8] **Question 1.** Recall that $\mathbb{Z}_7$ denotes the set $\{0, 1, 2, 3, 4, 5, 6\}$ together with the operations of addition and multiplication modulo 7. Recall that every non-zero element of $\mathbb{Z}_7$ has a multiplicative inverse modulo 7:

$$1 \cdot 1 \equiv 1 \pmod 7, \quad 2 \cdot 4 \equiv 1 \pmod 7, \quad 3 \cdot 5 \equiv 1 \quad (\text{mod } 7,) \quad 6 \cdot 6 \equiv 1 \pmod 7$$

Consider the following system of congruences:

$$\begin{cases} 3w + 5x + 5y + 2z & \equiv & 1 \pmod 7 \\ 2w + \ \ x + 3y + 5z & \equiv & 4 \pmod 7 \end{cases}$$

Using only the method of Gaussian elimination with back substitution, or the method of Gauss-Jordan elimination, from first year Linear Algebra, [row reduction in matrix form, *no* column operations] and *only* arithmetic in $\mathbb{Z}_7$, find all solutions to this system. Give your solution in vector form.

NOTE: It really was essential to work out this problem "modulo 7". Real number or rational arithmetic is wrong.

Solution: There are different pathways to the solution, but the row-reduced echelon form of the matrix is unique. Because of the precise statement of the question, column operations are not permitted.

The augmented matrix of the system is

$$\left|\begin{array}{cccc|c} 3 & 5 & 5 & 2 & 1 \\ 2 & 1 & 3 & 5 & 4 \end{array}\right| \qquad 5R_1$$

$$\left|\begin{array}{cccc|c} 1 & 4 & 4 & 3 & 5 \\ 2 & 1 & 3 & 5 & 4 \end{array}\right| \qquad R_2 - 2R_1$$

$$\left|\begin{array}{cccc|c} 1 & 4 & 4 & 3 & 5 \\ 0 & 0 & 2 & 6 & 1 \end{array}\right| \qquad 4R_2$$

$$\left|\begin{array}{cccc|c} 1 & 4 & 4 & 3 & 5 \\ 0 & 0 & 1 & 3 & 4 \end{array}\right| \qquad R_1 - 4R_2$$

$$\left|\begin{array}{cccc|c} 1 & 4 & 0 & 5 & 3 \\ 0 & 0 & 1 & 3 & 4 \end{array}\right|$$

So we take x as a parameter a and z as a parameter b and find

$$w = 3 + 2a + 2b \qquad y = 4 + 4b\,.$$

This is enough for the answer to this problem, but it is nicer to write the solution in vector-parametric form:

$$\begin{bmatrix} w \\ x \\ y \\ z \end{bmatrix} = \begin{bmatrix} 3 \\ 0 \\ 4 \\ 0 \end{bmatrix} + a \begin{bmatrix} 3 \\ 1 \\ 0 \\ 0 \end{bmatrix} + b \begin{bmatrix} 2 \\ 0 \\ 4 \\ 1 \end{bmatrix}$$

Remarks: [On elementary linear algebra] We can interpret our work over $\mathbb{Z}_7$ in exactly the same way we do when we work over $\mathbb{Q}$ or $\mathbb{R}$. There are two vector spaces here, over the field $\mathbb{Z}_7$: the four dimensional space $(\mathbb{Z}_7)^4$ and the two dimensional space $(\mathbb{Z}_7)^2$. The coefficient matrix is

$$A = \begin{bmatrix} 3 & 5 & 5 & 2 \\ 2 & 1 & 3 & 5 \end{bmatrix}$$

The row space of A and the null space of A are (complementary) subspaces of $(\mathbb{Z}_7)^4$. A nice basis for the row space consists of the non-zero rows of the row-reduced echelon form of A:

$$\{ \begin{bmatrix} 1 & 4 & 0 & 5 \end{bmatrix}, \begin{bmatrix} 0 & 0 & 1 & 3 \end{bmatrix} \}$$

and a basis for the null space of A is given by the vector coefficients of the parameters:

$$\left\{ \begin{bmatrix} 3 \\ 1 \\ 0 \\ 0 \end{bmatrix}, \begin{bmatrix} 2 \\ 0 \\ 4 \\ 1 \end{bmatrix} \right\}$$

The column space of A and the left null space of A are subspaces of $(\mathbb{Z}_7)^2$. Since "row rank equals column rank", the column space has dimension 2 and so the complementary subspace the left null space of A, has dimension 0. The standard basis for the column space is obtained by taking the columns of A that correspond to the "pivot" columns of the row-reduced echelon form of A:

$$\left\{ \begin{bmatrix} 3 \\ 2 \end{bmatrix}, \begin{bmatrix} 5 \\ 3 \end{bmatrix} \right\}$$

Question 2.

[2] (a) Find all Pythagorean triples where one of x, y, and z is equal to 17.

Solution: Since 17 is a prime, in fact the triples must be primitive.

Thus either $x = r^2 - s^2 = 17$ or $z = r^2 + s^2 = 17$. There are then only two solutions: $r = 9$, $s = 8$ giving the triple 17, 144, 145, and $r = 4$, $s = 1$ giving the triple 15, 8, 17.

[2] (b) Find all primitive Pythagorean triples where $y = 30$, if any.

Solution: So $2rs = 30$ and $rs = 15$, where $r > s > 0$ and r and s are relatively prime and incongruent modulo 2. But $rs = 15$ implies r and s are both odd, so there are no such primitive Pythagorean triples! **Remark**: There are two triples with $y = 30$: 224, 30, 226 and 16, 30, 34; but they are not primitive.

[4] **Question 3.** Prove that if $\langle x, y, z \rangle$ is a Pythagorean triple, then one of x, y, z is divisible by 3, and one of x, y, z is divisible by 5.

Proof: Suppose $x^2 + y^2 = z^2$, an equation in non-negative integers. Then if $3 \nmid x$ and $3 \nmid y$, then $x^2 \equiv y^2 \equiv 1 \pmod 3$ and so $z^2 \equiv 2 \pmod 3$. But 2 is not a square $\pmod 3$, so in fact one of x or y is divisible by 3.

If neither x nor y is divisible by 5, then $x^2 \equiv \pm 1 \pmod 5$ and $y^2 \equiv \pm 1 \pmod 5$ and so z^2 is congruent to one of $0, \pm 2 \pmod 5$. But 2 is not a square modulo 5, so $z \equiv 0 \pmod 5$. $\blacksquare$

Proof: A Pythagorean triple in general has the form

$$x = r^2 - s^2 \qquad y = 2rs \qquad z = r^2 + s^2 \qquad (r > s)$$

If neither r nor s is divisible by 3, that is, they are not congruent to 0 mod 3, so that y is not divisible by 3, then they are congruent to 1 or -1 mod 3. Thus either $r \equiv s \pmod 3$ or $r \equiv -s \pmod 3$; in either case $x = r^2 - y^2 \equiv 0 \pmod 3$.

If neither r nor s is divisible by 5, that is, they are not congruent to 0 mod 5, so that y is not divisible by 5, then r^2 and s^2 are each congruent to either 1 or -1 mod 5. If they are congruent to each other, then $x = r^2 - s^2 \equiv 0 \pmod 5$, and if they are congruent to opposites, then $z = r^2 + s^2 \equiv 0 \pmod 5$. $\blacksquare$

[4] **Question 4.** $g = 2$ is a primitive root modulo 19.

t	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18
g^t	2	4	8	16	13	7	14	9	18	17	15	11	3	6	12	5	10	1

Use this information to calculate the least residue modulo 19 of

(a) $4 \cdot 5 \cdot 7 \cdot 11 \cdot 15 \cdot 17$ (b) 12^{100}

(a) **Solution:**

$$4 \cdot 5 \cdot 7 \cdot 11 \cdot 15 \cdot 17 \equiv 2^2 2^{16} 2^6 2^{12} 2^{11} 2^{10} \equiv 2^{2+16+6+12+11+10} \pmod{19},$$

and $2 + 16 + 6 + 12 + 11 + 10 = 57 \equiv 3 \pmod{18}$, so

$$4 \cdot 5 \cdot 7 \cdot 11 \cdot 15 \cdot 17 \equiv 2^3 \equiv 8 \pmod{19}.$$

(b) **Solution:** $12^{100} \equiv (2^{15})^{100} = 2^{1500} \pmod{19}$, and $1500 \equiv 6 \pmod{18}$, so $12^{100} \equiv 2^6 \equiv 7 \pmod{19}$.