MATH 135 Algebra, Solutions to Assignment 8

1: Solve each of the following linear congruences.

(a) $5x \equiv 4 \pmod 7$

Solution: We make a table of values modulo 7.

x	0	1	2	3	4	5	6
$5x$	0	5	3	1	6	4	2

From the table we see that $5x \equiv 4 \pmod 7$ when $x \equiv 5 \pmod 7$.

(b) $40x \equiv 15 \pmod{65}$

Solution: We have $40x \equiv 15 \pmod{65}$ when $40x = 15 + 65k$ for some integer k, or equivalently when $40x + 65y = 15$ for some integer y. The Euclidean Algorithm gives

$$65 = 1 \cdot 40 + 25\ , \quad 40 = 1 \cdot 25 + 15\ , \quad 25 = 1 \cdot 15 + 10\ , \quad 15 = 1 \cdot 10 + 5\ , \quad 10 = 2 \cdot 5 + 0$$

so we have $\gcd(40, 65) = 5$. Then Back-Substitution gives the sequence

$$1\ , \quad -1\ , \ , \quad 2 \quad -3\ , \quad 5$$

so we have $40(5) + 65(-3) = 5$. Multiply both sides by $\frac{15}{5} = 3$ to get $40(15) + 65(-9) = 15$. Thus one solution to the given congruence is $x = 15$. Note that $\frac{65}{5} = 13$, so by the Linear Congruence Theorem, the general solution is $x \equiv 15 \equiv 2 \pmod{13}$. Equivalently, $x \equiv 2, 15, 28, 41$ or $54 \pmod{65}$.

(c) $391x \equiv 119 \pmod{1003}$

Solution: We have $391x \equiv 119 \pmod{1003}$ when $391x + 1003y = 119$ for some integer y. The Euclidean Algorithm gives

$$1003 = 2 \cdot 391 + 21\ , \quad 391 = 1 \cdot 221 + 170\ , \quad 221 = 1 \cdot 170 + 51\ , \quad 170 = 3 \cdot 51 + 17\ , \quad 51 = 3 \cdot 17 + 0$$

so $\gcd(391, 1003) = 17$. Back-Substitution then gives

$$1\ , \quad -3\ , \quad 4\ , \quad -7\ , \quad 18$$

so we have $391(18) + (1003)(-7) = 17$. Multiply both sides by $\frac{119}{17} = 7$ to get $391(126) + 1003(-49) = 119$. Thus one solution to the given congruence is $x = 126$. Note that $\frac{1003}{17} = 59$, so by the Linear Congruence Theorem, the general solution is $x \equiv 126 \equiv 8 \pmod{59}$.

2: (a) Find $[12]^{-1}$ in $\mathbf{Z}_{29}$.

Solution: We must find x such that $12x \equiv 1 \pmod{29}$, that is $12x + 29y = 1$ for some integer y. The Euclidean Algorithm gives

$$29 = 2 \cdot 12 + 5\ , \quad 12 = 2 \cdot 5 + 2\ , \quad 5 = 2 \cdot 2 + 1\ , \quad 2 = 2 \cdot 1 + 0$$

so $\gcd(12, 29) = 1$, and then Back-Substitution gives

$$1\ , \quad -2\ , \quad 5\ , \quad -12$$

so we have $12(-12) + 29(5) = 1$. One solution to the congruence is $x = -12$, so $[12]^{-1} = [-12] = [17]$ in $\mathbf{Z}_{29}$.

(b) Solve $[34]x = [18]$ in $\mathbf{Z}_{46}$.

Solution: For $x \in \mathbf{Z}$, to get $34x \equiv 18 \pmod{46}$, we need $34x + 46y = 18$ for some integer y. The Euclidean Algorithm gives

$$46 = 1 \cdot 34 + 12\ , \quad 34 = 2 \cdot 12 + 10\ , \quad 12 = 1 \cdot 10 + 2\ , \quad 10 = 5 \cdot 2 + 0$$

so $\gcd(10, 46) = 2$, and then Back-Substitution then gives

$$1\ , \quad -1\ , \quad 3\ , \quad -4$$

so we have $34(-4) + 46(3) = 2$. Multiply both sides by $\frac{18}{2} = 9$ to get $34(-36) + 46(27) = 18$. Thus one solution to the congruence is $x = -36$. Note that $\frac{46}{2} = 23$, so by the Linear Congruence Theorem, the general solution to the congruence is $x \equiv -36 \equiv 10 \pmod{23}$. Equivalently, $x \equiv 10$ or $33 \pmod{46}$. Thus for $x \in \mathbf{Z}_{46}$, there are two solutions to the given equation, namely $x = [10]$ and $x = [33]$.

(c) In $\mathbf{Z}_{20}$, solve the pair of simultaneous equations

$$[7]x + [12]y = [6]$$
$$[6]x + [11]y = [13]$$

Solution: Note that $[7]$ is invertible in $\mathbf{Z}_{20}$, indeed by inspection, we have $[7]^{-1} = [3]$. Multiply the first equation by $[3]$ to get $x + [16]y = [18]$, that is

$$x = [18] - [16]y = [4]y - [2]\,.$$

Put this into the second equation to get $[6]\big([4]y - [2]\big) + [11]y = [13]$, that is $[4]y - [12] + [11]y = [13]$, or equivalently $[15]y = [5]$. We have

$$[15]y = [5] \text{ in } \mathbf{Z}_{20} \iff 15y \equiv 5 \pmod{20} \iff 3y \equiv 1 \pmod{4} \iff y \equiv 3 \pmod{4}$$
$$\iff y = [3], [7], [11], [15] \text{ or } [19] \text{ in } \mathbf{Z}_{20}\,.$$

Put each of these values for y back in the equation $x = [4]y - [2]$ to get the solutions

$$(x, y) = \big([10], [3]\big), \big([6], [7]\big), \big([2], [11]\big), \big([18], [15]\big), \big([14], [19]\big)\,.$$

3: (a) Find the inverse of every invertible element in $\mathbf{Z}_{15}$.

Solution: The invertible elements are the elements $[a]$ with $\gcd(a, 15) = 1$, that is

$$[a] = [1]\ ,\ [2]\ ,\ [4]\ ,\ [7]\ ,\ [8]\ ,\ [11]\ ,\ [13]\ ,\ [14]\,.$$

Of course $[1]^{-1} = [1]$. We find a few multiples of $[2]$; we have $[2][2] = [4]$, $[2][4] = [8]$, $[2][7] = [14] = [-1]$. Since $[2][7] = [-1]$, we have $[2]^{-1} = [-7] = [8]$, $[8]^{-1} = [2]$, $[7]^{-1} = [-2] = [13]$ and $[13]^{-1} = [7]$. Also, we have $[4][4] = [16] = [1]$ so that $[4]^{-1} = [4]$, and $[11][11] = [-4][-4] = [4][4] = [1]$ so that $[11]^{-1} = [11]$, and $[14][14] = [-1][-1] = [1]$ so that $[14]^{-1} = [14]$. We summarize in the following table of inverses.

x	$[1]$	$[2]$	$[4]$	$[7]$	$[8]$	$[11]$	$[13]$	$[14]$
x^{-1}	$[1]$	$[8]$	$[4]$	$[13]$	$[2]$	$[11]$	$[7]$	$[14]$

(b) With the help of the following list of powers of 5 mod 23, solve $[11]x^{18} = [15]$ in $\mathbf{Z}_{23}$.

k	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21
5^k	1	5	2	10	4	20	8	17	16	11	9	22	18	21	13	19	3	15	6	7	12	14

Solution: Note that by Fermat's Little Theorem, the list of powers of 5 modulo 23 repeats every 22 terms, so for integers k and l we have $[5]^k = [5]^l$ in $\mathbf{Z}_{23} \iff k \equiv l \pmod{22}$. Also notice, from the given list, that every non-zero element in $\mathbf{Z}_{23}$ is of the form $[5]^m$ for some integer m. Clearly $x = [0]$ is not a solution to the equation $[11]x^{18} = [15]$ in $\mathbf{Z}_{23}$. Let x be any non-zero element in $\mathbf{Z}_{23}$, and write $x = [5]^m$. We have

$$\begin{aligned}[11]x^{18} = [15] &\iff [5]^9 x^{18} = [5]^{17} \iff x^{18} = [5]^{17-9} = [5]^8 \iff \left([5]^m\right)^{18} = [5]^8 \\ &\iff [5]^{18m} = [5]^8 \iff 18m \equiv 8 \pmod{22} \iff 9m \equiv 4 \pmod{11}\,.\end{aligned}$$

By inspection, one solution to the congruence $9m \equiv 4 \pmod{11}$ is given by $m = -2$, so the general solution is $m \equiv -2 \equiv 9 \pmod{11}$, or equivalently $m = 9$ or $20 \pmod{22}$. Thus the solutions to the given equation are $x = [5]^m$ where $m = 9$ or 20, that is $x = [11]$ or $[12]$.

4: (a) Find $17^{458} \pmod{13}$.

Solution: Since $17 \equiv 4 \pmod{13}$ we have $17^{458} \equiv 4^{458} \pmod{13}$. By Fermat's Little Theorem, the list of powers of 4 modulo 13 repeats every 12 terms, and we have $458 \equiv 2 \pmod{12}$, and so

$$17^{458} \equiv 4^{458} \equiv 4^2 \equiv 16 \equiv 3 \pmod{13}.$$

(b) Find $47^{38^{54}} \pmod{11}$.

Solution: Since $47 \equiv 3 \pmod{11}$ we have $47^{38^{54}} \equiv 3^{38^{54}} \pmod{11}$. We make a list of powers of 3 modulo 11.

k	0	1	2	3	4	5
3^k	1	3	9	5	4	1

We see that the list of powers of 3 modulo 11 repeats every 5 terms, so we calculate $38^{54} \pmod{5}$. Since $38 \equiv 3 \pmod{5}$ we have $38^{54} \equiv 3^{54} \pmod{5}$. We make a list of powers of 3 modulo 5.

k	0	1	2	3	4
3^k	1	3	4	2	1

We see that the list repeats every 4 terms (this also follows from Fermat's Little Theorem), and we have $54 \equiv 2 \pmod{4}$, and so $3^{54} \equiv 3^2 \equiv 4 \pmod{5}$. Thus

$$47^{38^{54}} \equiv 3^{38^{54}} \equiv 3^{3^{54}} \equiv 3^{3^2} \equiv 3^4 \equiv 4 \pmod{11}.$$

(c) Find $\sum_{k=1}^{300} k^k \pmod{7}$.

Solution: We begin by making a table of powers modulo 7.

k	0	1	2	3	4	5	6
2^k	1	2	4	1	2	4	1
3^k	1	3	2	6	4	5	1
4^k	1	4	2	1	4	2	1
5^k	1	5	4	6	2	3	1
6^k	1	6	1	6	1	6	1

For a non-negative integer n, let $S(n) \equiv n^0 + n^1 + n^2 + n^3 + n^4 + n^5 \pmod{7}$. Using the above table, we find that $S(2) = S(3) = S(4) = S(5) = S(6) = 0$. We have

$$\begin{aligned}
\sum_{k=1}^{300} k^k &= 1^1 + 2^2 + 3^3 + \cdots + 300^{300} \\
&\equiv \left(1^1 + 2^2 + \cdots + 6^6\right) + \left(0^7 + 1^8 + 2^9 + \cdots + 6^{13}\right) + \left(0^{14} + 1^{15} + 2^{16} + \cdots + 6^{20}\right) \\
&\quad + \cdots + \left(0^{294} + 1^{295} + 2^{296} + \cdots + 6^{300}\right) \pmod{7} \\
&\equiv \left(0^7 + 0^{14} + \cdots + 0^{294}\right) + \left(1^1 + 1^8 + 1^{15} + \cdots + 1^{295}\right) + \left(2^2 + 2^9 + 2^{16} + \cdots + 2^{296}\right) \\
&\quad + \cdots + \left(6^6 + 6^{13} + 6^{20} + \cdots + 6^{300}\right) \pmod{7}.
\end{aligned}$$

The term $\left(1^1 + 1^8 + 1^{15} + \cdots + 1^{295}\right)$ is the sum of 43 copies of 1, so it is equal to $43 \equiv 1 \pmod{7}$. Consider the term $\left(2^2 + 2^9 + 2^{16} + \cdots + 2^{296}\right)$. Since the list of powers of 2 repeats every 6 terms, we have

$$\begin{aligned}
\left(2^2 + 2^9 + 2^{16} + \cdots + 2^{296}\right) &= \left(2^2 + (2^3 + 2^4 + 2^5 + 2^0 + 2^1 + 2^2) + (2^3 + 2^4 + 2^5 + 2^0 + 2^1 + 2^2)\right. \\
&\quad \left. + \cdots + (2^3 + 2^4 + 2^5 + 2^0 + 2^1 + 2^2)\right) \\
&= 2^2 + 7\,S(2) = 2^2 + 7 \cdot 0 = 2^2.
\end{aligned}$$

Similarly, $\left(3^3 + 3^{10} + 3^{17} + \cdots + 3^{297}\right) = 3^3$ and $\left(4^4 + 4^{11} + 4^{18} + \cdots + 4^{298}\right) = 4^4$ and so on. Thus

$$\sum_{k=1}^{300} k^k = 0 + 1 + 2^2 + 3^3 + 4^4 + 5^5 + 6^6 \equiv 0 + 1 + 4 + 6 + 4 + 3 + 1 \equiv 5 \pmod{7}.$$

5: For this problem, you may find it useful to read some of sections 9.1 and 9.9 in the text. In particular in section 9.1, have a look at the example involving long division in $\mathbf{Z}_5$ on page 231, and see the Remainder Theorem 9.12 and the Factor Theorem 9.14 on page 232, and in section 9.9, look at example 9.92 on page 260. It is also worth noticing that Theorem 9.17 in section 9.1 does not always hold for polynomials over $\mathbf{Z}_n$.

(a) Solve $x^2+3x+2 \equiv 0 \pmod 6$, then find two different ways to factor the polynomial $f(x) = x^2+[3]x+[2]$ over $\mathbf{Z}_6$.

Solution: We make a table of values modulo 6.

x	0	1	2	3	4	5
x^2	0	1	4	3	4	1
x^2+3x+2	2	0	0	2	0	0

We see that $x^2 + 3x + 2 \equiv 0 \pmod 6$ when $x \equiv 1, 2, 4$ or $5 \pmod 6$. Thus the degree 2 polynomial $f(x) = x^2 + [3]x + [2]$ has the four roots $x = [1], [2], [4], [6]$ in $\mathbf{Z}_6$. Dividing $f(x)$ by $\big(x - [1]\big)$ gives

$$f(x) = \big(x - [1]\big)\big(x + [4]\big) = \big(x - [1]\big)\big(x - [2]\big)$$

and dividing $f(x)$ by $\big(x - [4]\big)$ gives

$$f(x) = \big(x - [4]\big)\big(x + [1]\big) = \big(x - [4]\big)\big(x - [5]\big)\,.$$

(b) Solve $x^2 + 2x + 26 \equiv 0 \pmod{125}$, then find two ways to factor $f(x) = x^2 + [2]x + [26]$ over $\mathbf{Z}_{125}$.

Solution: Note that if $x^2 + 2x + 26 \equiv 0 \pmod{125}$ then we also have $x^2 + 2x + 26 \equiv 0 \pmod{25}$ and $x^2+2x+26 \equiv 0 \pmod 5$. Let us begin by solving $x^2+2x+26 \equiv 0 \pmod 5$, that is $x^2+2x+1 \equiv 0 \pmod 5$. We make a table of values modulo 5.

x	0	1	2	3	4
x^2	0	1	4	4	1
x^2+2x+1	1	4	4	1	0

We see that $x^2 + 2x + 1 \equiv 0 \pmod 5$ when $x = 4 \pmod 5$.

Next we solve $x^2+2x+26 \equiv 0 \pmod{25}$, that is $x^2+2x+1 \equiv 0 \pmod{25}$. To have $x^2+2x+1 \equiv 0 \pmod{25}$ we must have $x^2 + 2x + 1 \equiv 0 \pmod 5$, so we must have $x \equiv 4 \pmod 5$, that is $x = 4 + 5k$ for some integer k. When $x = 4 + 5k$ we have

$$x^2 + 2x + 1 \equiv (4 + 5k)^2 + 2(4 + 5k) + 1 \equiv 16 + 40k + 25k^2 + 8 + 10k + 1 \equiv 25k^2 + 50k + 25 \equiv 0 \pmod{25}\,.$$

Thus $x^2 + 2x + 26 \equiv 0 \pmod{25}$ whenever $x \equiv 4 \pmod 5$.

Finally, we solve $x^2 + 2x + 26 \equiv 0 \pmod{125}$. To have $x^2 + 2x + 26 \equiv 0 \pmod{125}$, we must have $x^2 + 2x + 26 \equiv 0 \pmod{25}$, so we must have $x \equiv 4 \pmod 5$. When $x = 4 + 5k$ we have

$$x^2 + 2x + 26 \equiv (4 + 5k)^2 + 2(4 + 5k) + 26 \equiv 16 + 40k + 25k^2 + 8 + 10k + 26 \equiv 25k^2 + 50k + 50 \pmod{125}\,.$$

Thus

$$x^2 + 2x + 26 \equiv 0 \pmod{125} \iff 25k^2 + 50k + 50 \equiv 0 \pmod{125} \iff k^2 + 2k + 2 \equiv 0 \pmod 5\,.$$

We make a table of values modulo 5.

k	0	1	2	3	4
k^2+2k+2	2	0	0	2	1

We see that $k^2 + 2k + 2 \equiv 0 \pmod 5$ when $k \equiv 1$ or $2 \pmod 5$, that is $k = 1 + 5l$ or $k = 2 + 5l$ for some integer l. When $k = 1 + 5l$ we have $x = 4 + 5k = 4 + 5(1 + 5l) = 9 + 25l$, and when $k = 2 + 5l$ we have $x = 4 + 5k = 4 + 5(2 + 5l) = 14 + 25l$. Thus the solutions are $x = 9$ or $14 \pmod{25}$, that is

$$x = 9\ ,\ 14\ ,\ 34\ ,\ 39\ ,\ 59\ ,\ 64\ ,\ 84\ ,\ 89\ ,\ 109\ ,\ 114 \pmod{125}\,.$$

Thus the degree two polynomial $f(x) = x^2 + [2]x + [26]$ has 10 roots in $\mathbf{Z}_{125}$. We can factor $f(x)$ in many different ways, indeed we have

$$f(x) = \big(x-[9]\big)\big(x-[114]\big) = \big(x-[14]\big)\big(x-[109]\big) = \big(x-[34]\big)\big(x-[89]\big) = \big(x-[39]\big)\big(x-[84]\big) = \big(x-[59]\big)\big(x-[64]]\big)\,.$$