PMATH 340 Number Theory, Solutions to Assignment 2

1: (a) Find all possible pairs of decimal digits (a,b) such that $99\big|38a91b$.

Solution: Note that $99\big|38a91b$ implies that $9\big|38a91b$ and $11\big|38191b$. We have

$$9\big|38a91b \Longrightarrow 9\big|(3+8+a+9+1+b) \Longrightarrow a+b=6 \text{ mod } 9 \Longrightarrow a+b=6 \text{ or } 15\,,$$

and

$$11\big|38a91b \Longrightarrow 11\big|(3-8+a-9+1-b) \Longrightarrow a-b=2 \text{ mod } 11 \Longrightarrow a-b=2 \text{ or } -9\,.$$

The only pair (a,b) with $a-b=-9$ is the pair $(a,b)=(0,9)$, but for this pair we have $a+b=9$, so it does not satisfy the condition that $a+b=6$ or 15. The only pairs (a,b) with $a-b=2$ are the pairs $(a,b)=(2,0),(3,1),(4,2),\cdots,(9,7)$. Of these 8 pairs, only the pair $(a,b)=(4,2)$ satisfies the condition $a+b=6$ or 15. Thus $(a,b)=(4,2)$ is the only such pair.

(b) Let $n=a_0+a_1\cdot 1000+a_2\cdot 1000^2+\cdots+a_\ell\cdot 1000^\ell$ where $a_\ell\neq 0$ and for each i we have $a_i\in\{0,1,\cdots,999\}$. Show that for $d=7$, 11 and 13 we have

$$d\big|n \iff d\big|\big(a_0-a_1+a_2-a_3+\cdots+(-1)^\ell a_\ell\big)\,.$$

Solution: Let $n=a_0+a_1\cdot 1000+a_2\cdot 1000^2+\cdots+a_l\cdot 1000^l$ where $a_l\neq 0$ and for each i we have $0\le a_i<1000$. Notice that $1001=7\cdot 11\cdot 13$, so for $d=7$, 11 or 13, we have $1000=-1$ mod d, and so

$$\begin{aligned} n &= a_0+a_1\cdot 1000+a_2\cdot 1000^2+\cdots+a_l\cdot 1000^l \\ &= a_0+a_1(-1)+a_2(-1)^2+\cdots+a_l(-1)^l \mod d \\ &= a_0-a_1+a_2-a_3+\cdots+(-1)^l a_l \mod d \end{aligned}$$

and

$$\begin{aligned} d\big|n &\iff n=0 \text{ mod } d \\ &\iff a_0-a_1+a_2-a_3+\cdots+(-1)^l a_l=0 \mod d \\ &\iff d\big|\big(a_0-a_1+a_2-a_3+\cdots+(-1)^l a_l\big)\,. \end{aligned}$$

(c) Show that it is not possible to rearrange the digits of the number 51328167 to form a perfect square or a perfect cube or any higher perfect power.

Solution: If we rearrange the digits of 51328167 in any way, to form a number a, then we have $3\big|a$ since $5+1+3+2+8+1+6+7=33=0$ mod 3, but $9\not|a$ since $33\neq 0$ mod 9. Thus the exponent of 3 in the prime factorization of a is equal to 1, so a cannot be a square or a cube or any higher perfect power.

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

Solution: We must find x such that $12x = 1 \bmod 29$, 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 the sequence

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

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

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

Solution: For $x \in \mathbb{Z}$, to get $34x = 18 \bmod 46$, 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 $x = -36 = 10 \bmod 23$. Equivalently, $x = 10$ or $33 \bmod 46$. Thus for $x \in \mathbb{Z}_{46}$, there are two solutions to the given equation, namely $x = 10$ and $x = 33$.

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

$$\begin{aligned} 7x + 12y &= 6 \\ 6x + 11y &= 13 \end{aligned}$$

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

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

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

$$\begin{aligned} 15y = 5 \text{ in } \mathbb{Z}_{20} &\iff 15y = 5 \bmod 20 \iff 3y = 1 \bmod 4 \iff y = 3 \bmod 4 \\ &\iff y = 3, 7, 11, 15 \text{ or } 19 \text{ in } \mathbb{Z}_{20}\,. \end{aligned}$$

Put each of these values for y back in the equation $x = 4y - 2$ 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) Solve the pair of congruences $5x = 9 \bmod 14$ and $17x = 3 \bmod 30$.

Solution: We have $5x = 9 \bmod 14 \iff 5x \in \{\cdots, -5, 9, 23, \cdots\}$. By inspection, one solution to the first congruence is given by $x = -1$ and, since $\gcd(5, 14) = 1$, the general solution is given by $x = -1 \bmod 14$. To get $17x = 3 \bmod 30$ we need $17x + 30y = 3$ for some $y \in \mathbb{Z}$. The Euclidean Algorithm gives

$$30 = 1 \cdot 17 + 13\ ,\ 17 = 1 \cdot 13 + 4\ ,\ 13 = 3 \cdot 4 + 1$$

so that $d = \gcd(17, 30) = 1$, and then Back-Substitution gives the sequence

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

so that $17(-7) + 30(4) = 1$. Multiply by 3 to get $17(-21) + 30(12) = 3$, and so one solution to the second congruence is $x = -21$ and the general solution is $x = -21 = 9 \bmod 30$. Thus the two given congruences are equivalent to the two congruences $x = -1 \bmod 14$ (1) and $x = 9 \bmod 30$ (2). To solve these two congruences we try to find $k, \ell \in \mathbb{Z}$ so that $x = -1 + 14k = 9 + 30\ell$. We need $14k - 30\ell = 10$. Divide by 2 to get $7k - 15\ell = 5$. By inspection, one solution is given by $(k, \ell) = (-10, -5)$. Put $k = -10$ into the equation $x = -1 + 14k$ toget $x = -141$, and so $x = -141$ is one solution to the pair of congruences (1) and (2). Since $\gcd(14, 30) = 2$ so that $\mathrm{lcm}(14, 30) = \frac{14 \cdot 30}{2} = 210$, by the CRT (the Chinese Remainder Theorem) the general solution is $x = -141 \bmod 210$, or equivalently $x = 69 \bmod 210$.

(b) Solve the congruence $x^2 + x = 38 \bmod 72$.

Solution: Note that $72 = 8 \cdot 9$. Working modulo 8, we have $38 = 6$, and we have the following table of values

x	0	1	2	3	4	5	6	7
x^2	0	1	4	1	0	1	4	1
$x^2 + x$	0	1	6	4	4	6	2	0

Thus we must have $x = 2$ or $5 \bmod 8$. Also, working modulo 9 we have $38 = 2$ and we have the following table of values

x	0	1	2	3	4	5	6	7	8
x^2	0	1	4	0	7	7	0	4	1
$x + x^2$	0	2	6	3	2	3	6	2	0

and so we must have $x = 1 \bmod 3$. By one solution by inspection then applying the CRT, we have

$$(x = 2 \bmod 8 \text{ and } x = 1 \bmod 3) \iff x = 10 \bmod 24\ , \text{ and}$$
$$(x = 5 \bmod 8 \text{ and } x = 1 \bmod 3) \iff x = 13 \bmod 24\,.$$

Thus the solution is $x = 10$ or $13 \bmod 24$.

4: Chinese generals used to count their troops by telling them to form groups of some size n, and then counting the number of troops left over. Suppose there were 5000 troops before a battle, and after the battle it was found that when the troops formed groups of 5 there was 1 left over, when they formed groups of 7 there were none left over, when they formed groups of 11 there were 6 left over, and when they formed groups of 12 there were 5 left over. How many troops survived the battle?

Solution: We must solve the system of congruences

$$\begin{aligned} x &= 1 \bmod 5 \\ x &= 0 \bmod 7 \\ x &= 6 \bmod 11 \\ x &= 5 \bmod 12\,. \end{aligned}$$

Note that $x = 21$ is a solution to the first pair of congruences so by the CRT (the Chinese Remainder Theorem), the general solution to the first pair is $x = 21 \bmod 35$. Also note that $x = 17$ is a solution to the second pair of congruences, so by the CRT, the general solution is $x = 17 \bmod 132$. Thus we must solve the pair of congruences

$$\begin{aligned} x &= 21 \bmod 35 \\ x &= 17 \bmod 132\,. \end{aligned}$$

For x to be a solution we need $x = 21 + 35r$ and $x = 17 + 132s$ for some integers r and s, so we must have $21 + 35r = 17 + 132s$, that is $35r - 132s = -4$. The Euclidean Algorithm gives

$$132 = 3 \cdot 35 + 27\ ,\quad 35 = 1 \cdot 27 + 8\ ,\quad 27 = 3 \cdot 8 + 3\ ,\quad 8 = 2 \cdot 3 + 2\ ,\quad 3 = 1 \cdot 2 + 1$$

so we have $\gcd(35, 132) = 1$, and then Back-Substitution gives

$$1\ ,\quad -1\ ,\quad 3\ ,\quad -10\ ,\quad 13\ ,\quad -49$$

and so we have $(35)(-49) - (132)(-13) = 1$. Multiply both sides by -4 to get $(35)(196) - (132)(52) = -4$. Thus one solution to the linear diophantine equation $35r - 132s = -4$ is given by $(r, s) = (196, 52)$, and by the Linear Diophantine Equation Theorem, the general solution is $(r, s) = (196, 52) + k(132, 35)$, $k \in \mathbb{Z}$, so we have $r = 196 = 64 \bmod 132$. Thus one solution to the above pair of congruences (which is equivalent to the original system of 4 congruences) is $x = 21 + 35r = 21 + (35)(64) = 2261$. Note that $35 \cdot 132 = 4620$, so by the CRT, the general solution to the pair of congruneces is

$$x = 2261 \bmod 4620\,.$$

Since $2261 - 4620 < 0$ and $2261 + 4620 > 5000$, there must be 2261 troops remaining after the battle.